McAfee®

Internet Security Suite 2007

使用手冊

內容

McAfee Network Manager 47

McAfee VirusScan 65

McAfee Personal Firewall 105

第 1 章

McAfee Internet Security

McAfee Internet Security Suite 會保護您的身份與電腦免於線上威脅，同時提供重要檔案的自動備份，讓您享受無憂的網際網路體驗。McAfee 值得信賴的保護永遠開啓、隨時更新，並且隨時保護您的網際空間，因此您可以安全地漫遊、購物、使用網路銀行、收發電子郵件、傳送即時訊息以及下載檔案。McAfee 還使用重新設計的 McAfee SecurityCenter，讓您可以輕易地檢視安全性狀態、掃描病毒與間諜軟體，並確保您產品保持最新狀態。此外，訂閱後，您還會自動收到最新的 McAfee 軟體與更新。

Internet Security 包含下列程式：

- SecurityCenter
- Privacy Service
- Shredder
- VirusScan
- Personal Firewall
- SpamKiller
- Data Backup
- Network Manager
- EasyNetwork (只限 3 位使用者的授權)
- SiteAdvisor

第　2　章

McAfee SecurityCenter

McAfee SecurityCenter 是一種簡單易用的環境，可以讓 McAfee 使用者啓動、管理及設定其安全性訂閱。

SecurityCenter 也是病毒警示、產品資訊、支援、訂閱資訊，以及 McAfee 網站所提供之工具與新聞存取的資訊來源。

在本章中

功能

McAfee SecurityCenter 提供了下列的新功能及優點：

重新設計的保護狀態

輕鬆地檢視電腦的安全性狀態、檢查是否有更新並修正潛在的安全性問題。

持續更新與升級

自動安裝每日更新。在訂購期間，每當有新版的 McAfee 軟體時，您都可以自動且免費取得，確保您永遠擁有最新的保護。

即時警示

安全性警示會通知您緊急的病毒爆發和安全性威脅，並提供移除、消除或深入瞭解該威脅的回應選項。

便利的保護

各種續訂選項可讓您的 McAfee 保護永遠保持最新。

效能工具

移除不使用的檔案、重組使用過的檔案，並使用系統還原以使電腦的執行保持在顛峰效能。

真實的線上協助

透過網際網路交談、電子郵件與電話，獲得來自 McAfee 電腦安全性專家的支援。

安全漫遊保護

如果安裝 McAfee SiteAdvisor 瀏覽器外掛程式，便能對您所造訪或是在 Web 搜尋結果中出現的網站進行評等，以幫助您防止間諜軟體、垃圾郵件、病毒及線上騙局。您可檢視詳細的安全評等，評等會顯示網站針對電子郵件作法、下載、線上聯盟，以及例如快顯視窗及協力廠商追蹤 cookie 等困擾的網站測試經過。

第　3　章

使用 SecurityCenter

您可從工作列最右邊 Windows 通知區域中的 McAfee SecurityCenter 圖示，或從 Windows 桌面來執行 SecurityCenter。

開啓 SecurityCenter 時，[首頁] 窗格會顯示電腦的安全性狀態，並能讓您快速存取更新、掃描 (若已安裝 McAfee VirusScan)，及其他常見工作：

標頭

說明

檢視程式說明檔。

左欄位

更新

更新產品，確保免受最新的威脅攻擊。

掃描

如果已安裝 McAfee VirusScan，您可對電腦執行手動掃描。

常見工作

執行常見工作，包含回到 [首頁] 窗格、檢視最近的事件、管理電腦網路 (如果您位於具有此網路之管理功能的電腦上)，以及維護電腦。如果已安裝 McAfee Data Backup，您還可以備份資料。

安裝的元件

查看正在保護電腦安全的安全性服務。

主要窗格

保護狀態

在 [我是否受到保護?] 下，可以查看電腦保護狀態的整體層級。在其下方，可以依保護類別及類型來檢視狀態分析。

SecurityCenter 資訊

查看上次電腦更新的時間、上次掃描的時間 (如果已安裝 McAfee VirusScan)，以及訂閱到期的時間。

在本章中

瞭解 SecurityCenter 圖示

SecurityCenter 的圖示會出現在工作列最右邊的 Windows 通知區域中。使用這些圖示可以查看電腦是否受到完全的保護、檢視進行中的掃描狀態 (如果已安裝 McAfee VirusScan)、檢查更新、檢視最近的事件、維護電腦及取得 McAfee 網站的支援。

開啓 SecurityCenter 並使用其他功能

當 SecurityCenter 在執行中時，SecurityCenter M 圖示 會出現在工作列最右邊的 Windows 通知區域中。

若要開啓 SecurityCenter 或使用其他功能：

- 在主要 SecurityCenter 圖示上按一下滑鼠右鍵，再按下列其中一項：
  - 開啓 SecurityCenter
  - 更新
  - 快速連結

    子功能表包含 [首頁]、[檢視最近的事件]、[管理網路]、[維護電腦] 及 [備份與還原檔案] (若已安裝) 的連結。
  - 確認訂閱

    (當有一個或更多的產品訂閱過期時，便會顯示此項目)。
  - 升級中心
  - 客戶支援

檢查保護狀態

如果您的電腦未受到完全的保護，保護狀態圖示 會出現在工作列最右邊的 Windows 通知區域中。根據保護狀態的不同，圖示可能為紅色或黃色。

若要檢查保護狀態：

- 按一下保護狀態圖示以開啓 SecurityCenter，並修復任何問題。

檢查更新狀態

如果您正在檢查更新，更新圖示 會出現在工作列最右邊的 Windows 通知區域中。

若要檢查更新狀態：

- 指向更新圖示，在工具提示中檢視更新狀態。

瞭解保護狀態

電腦的整體安全保護狀態會顯示於 SecurityCenter 中的 [我是否受到保護?] 下方。

保護狀態會通知您電腦是否受到完全的保護，可防止最新的安全性威脅，或是否有需要注意的問題及解決方法。當一個問題影響到一個以上的保護類別時，修復此問題就會讓多個類別回復到完全保護的狀態。

一些會影響保護狀態的因素包括外部安全性威脅、電腦上安裝的安全性產品、存取網際網路的產品，以及這些安全性及網際網路產品的設定方式。

依預設，如果未安裝「垃圾郵件保護」或「內容封鎖」，則會自動略過這些不重要的保護問題，而且不會在整體保護狀態中進行追蹤。不過，如果保護問題之後有一個 [略過] 連結，您可以在確定不要修復此問題的時候，選擇略過。

我是否受到保護?

在 SecurityCenter 中的 [我是否受到保護?] 下，查看您電腦保護狀態的整體層級：

- 如果電腦受到完全的保護 (綠色)，則會顯示 [是]。
- 如果電腦只受到部份保護 (黃色) 或未受保護 (紅色)，則會顯示 [否]。

若要自動解決大多數的保護問題，請按一下保護狀態旁的 [修復]。然而如果一或多個問題持續發生且需要您的回應，請按一下問題後的連結以採取建議的動作。

瞭解保護類別及類型

您可以在 SecurityCenter 中的 [我是否受到保護?] 底下，檢視由下列保護類別及類型組成的狀態分析：

- 電腦與檔案
- 網際網路與網路
- 電子郵件與即時訊息
- 未成年保護

SecurityCenter 中顯示的保護類型會依安裝的產品而不同。例如，如果安裝了 McAfee Data Backup 軟體，會顯示個人電腦健全狀態保護類型。

如果某個類別沒有任何保護問題，其狀態會是綠色。如果您按一下綠色類別，右方會出現已啓用的保護類型清單，接者是已略過問題的清單。若沒有任何問題，則會顯示防毒忠告。您也可以按一下 [設定] 來變更類別選項。

如果某個類別內的所有保護類型都是綠色，則該類別的狀態便是綠色。同樣的，如果所有保護類別都是綠色，則整體的保護狀態也會是綠色。

若任何保護類別爲黃色或紅色狀態，您可修復或略過來解決保護問題，將狀態變更爲綠色。

瞭解電腦及檔案保護

電腦及檔案保護類別由下列保護類型組成：

- **病毒保護** -- 即時掃描保護會保護您的電腦，對抗病毒、蠕蟲、特洛伊木馬病毒、可疑的指令碼、混合攻擊及其他威脅。它會在您或您的電腦存取檔案 (包括 .exe 壓縮檔、開機磁區、記憶體及重要檔案) 時，自動掃描並嘗試清除檔案中的病毒。
- **間諜軟體保護** -- 間諜軟體保護能夠迅速地偵測、封鎖，並移除間諜軟體、廣告軟體及其他潛在無用的程式，這些程式可能不經允許就收集並傳輸您的私人資料。
- **SystemGuard** -- SystemGuard 會偵測您電腦的變更，並在發生變更時警示您。然後您可以檢閱這些變更並決定是否加以允許。
- **Windows 保護** -- Windows 保護會提供您電腦上的 Windows Update 狀態。如果已安裝 McAfee VirusScan，也同時提供緩衝區溢位保護。

外部的病毒威脅是影響電腦及檔案保護的因素之一。例如，如果爆發病毒，您的防毒軟體能夠保護您嗎？其他因素還包括防毒軟體的設定，及您是否以最新的病毒偵測簽章檔不時地更新軟體，以保護電腦抵禦最新威脅。

開啓電腦與檔案設定窗格

當 [電腦與檔案] 下沒有任何問題時，您可從資訊窗格開啓設定窗格。

若要開啓 [電腦與檔案] 設定窗格：

1 在 [首頁] 窗格中，按一下 [電腦與檔案]。

2 在右窗格中，按一下 [設定]。

瞭解網際網路及網路保護

網際網路與網路保護類別由下列保護類型所組成：

- **防火牆保護** -- 防火牆保護可幫助電腦抵禦入侵及無用的網路流量。它有助於管理入埠及出埠網際網路連線。
- **無線保護** -- 無線保護可幫助家用無線網路抵禦入侵及資料攔截。然而，如果您目前連線到外部無線網路，則對您的保護會根據該網路的安全性層級而定。
- **Web 瀏覽保護** -- Web 瀏覽保護會在您瀏覽網際網路時，隱藏電腦上的廣告、快顯視窗及 Web 錯誤。
- **網路釣魚保護** -- 網路釣魚保護有助於封鎖詐騙網站，這些網站通常會透過電子郵件與即時訊息中的超連結、快顯視窗及其他來源，企圖獲取個人資訊。
- **個人資訊保護** -- 個人資訊保護會封鎖在網際網路上散佈敏感及機密資訊。

開啓 [網際網路與網路] 設定窗格

當 [網際網路與網路] 下沒有任何問題時，您可從資訊窗格開啓設定窗格。

若要開啓 [網際網路與網路] 設定窗格：

1. 在 [首頁] 窗格中，按一下 [網際網路與網路]。
2. 在右窗格中，按一下 [設定]。

瞭解電子郵件及即時訊息保護

電子郵件及即時訊息保護類別由下列保護類型所組成：

- **電子郵件保護** -- 電子郵件保護會自動掃描，並嘗試清除入埠及出埠電子郵件及附件中的病毒、間諜軟體及潛在的威脅。
- **垃圾郵件保護** -- 垃圾郵件保護有助於封鎖無用的電子郵件進入您的收件匣。
- **即時訊息保護** -- 即時訊息 (IM) 保護會自動掃描，並嘗試清除入埠即時訊息附件中的病毒、間諜軟體及潛在的威脅。它也會封鎖即時訊息用戶端，不准透過網際網路交換無用內容或個人資訊。
- **安全漫遊保護** -- 如果安裝 McAfee SiteAdvisor 瀏覽器外掛程式，便能將您造訪或是在 Web 搜尋結果中出現的網站進行評等，來幫助您防止間諜軟體、垃圾郵件、病毒及線上騙局。您可檢視詳細的安全評等，評等會顯示網站針對電子郵件作法、下載、線上聯盟，以及例如快顯視窗及協力廠商追蹤 cookie 等困擾的網站測試經過。

開啓 [電子郵件與即時訊息] 設定窗格

當 [電子郵件與即時訊息] 下沒有任何問題時，您可從資訊窗格開啓設定窗格。

若要開啓 [電子郵件與即時訊息] 設定窗格：

1 在 [首頁] 窗格中，按一下 [電子郵件與即時訊息]。

2 在右窗格中，按一下 [設定]。

瞭解未成年保護

未成年保護類別包含此保護類型：

- **未成年保護 --** 「內容封鎖」能夠藉由封鎖可能有害的網站，防止使用者檢視無用的網際網路內容。也能夠監視並限制使用者的網際網路活動及使用情形。

開啓 [未成年保護] 設定窗格

當 [未成年保護] 下沒有任何問題時，您可從資訊窗格開啓設定窗格。

若要開啓 [未成年保護] 設定窗格：

1 在 [首頁] 窗格中，按一下 [未成年保護]。

2 在右窗格中，按一下 [設定]。

修復保護問題

大部份的保護問題都可自動解決。然而，如果一或多個問題持續發生，您就必須予以解決。

自動修復保護問題

大部份的保護問題都可自動解決。

若要自動修復保護問題：

- 按一下保護狀態旁的 [修復]。

手動修復保護問題

如果未自動解決一或多個保護問題，請按一下問題後的連結以採取建議的動作。

若要手動修復保護問題：

- 執行下列任一項：
  - 如果電腦超過 30 天都未執行完整掃描，請按一下主要保護狀態左邊的 [掃描] 來執行手動掃描。(如已安裝 McAfee VirusScan，就會出現此項目)。
  - 如果您的病毒偵測簽章 (DAT) 檔已過期，請按一下主要保護狀態左邊的 [更新] 來更新保護。
  - 如果未安裝程式，請按一下 [請取得完整的保護] 以進行安裝。
  - 如果程式遺失元件，請重新安裝。
  - 如果必須註冊程式才能取得完整的保護，請按一下 [立即註冊] 以進行註冊 (如果一或多個程式過期，則會顯示此項目)。
  - 如果程式過期，請按一下 [請立即確認訂購] 來檢查帳戶狀態 (如果一或多個程式過期，則會顯示此項目)。

檢視 SecurityCenter 資訊

SecurityCenter 資訊會在保護狀態窗格底部，供您存取 SecurityCenter 選項，並顯示 McAfee 產品上次更新、上次掃描 (若已安裝 McAfee VirusScan)，及訂閱過期的相關資訊。

開啓 [SecurityCenter 設定] 窗格

爲了方便使用，您可從 [首頁] 窗格開啓 [SecurityCenter 設定] 窗格來變更選項。

若要開啓 [SecurityCenter 設定] 窗格：

- 在 [首頁] 窗格的 [SecurityCenter 資訊] 底下，按一下 [設定]。

檢視已安裝產品的資訊

您可檢視已安裝產品的清單，其中會顯示產品版本號碼及上次更新時間。

若要檢視 McAfee 產品資訊：

- 在 [首頁] 窗格的 [SecurityCenter 資訊] 底下，按一下 [檢視詳細資料] 以開啓產品資訊視窗。

使用進階功能表

首次開啓 SecurityCenter 時，[基本功能表] 會出現在左邊的欄位中。若您是進階使用者，可按一下 [進階功能表] 就地開啓更詳細的命令功能表。爲了方便使用，下次開啓 SecurityCenter 就會顯示上次使用過的功能表。

進階功能表包含下列項目：

- 首頁
- 報告與記錄 (包含最近的事件清單，及過去 30、60 及 90 天內依類型排列的記錄)
- 設定
- 還原
- 工具

第 4 章

設定 SecurityCenter 選項

SecurityCenter 可顯示電腦的整體安全保護狀態、讓您建立 McAfee 使用者帳戶、自動安裝最新的產品更新，並在大範圍病毒爆發、安全性威脅及產品更新時自動通知您。

在 [SecurityCenter 設定] 窗格中，您可變更下列功能的 SecurityCenter 選項：

- 保護狀態
- 使用者
- 自動更新
- 警示

在本章中

設定保護狀態

電腦的整體安全保護狀態會在 SecurityCenter 中的 [我是否受到保護?] 底下顯示。

保護狀態會通知您電腦是否受到完全的保護，可防禦最新的安全性威脅，或是否有需要注意的問題及解決方法。

依預設，如果未安裝「垃圾郵件保護」或「內容封鎖」，則會自動略過這些不重要的保護問題，而且不會在整體保護狀態中進行追蹤。不過，如果保護問題之後有一個 [略過] 連結，您可以在確定不要修復此問題的時候，選擇略過。如果您之後決定要修復上次略過的問題，可將問題併入保護狀態中以進行追蹤。

設定略過的問題

您可併入或排除電腦整體保護狀態所追蹤的問題。如果保護問題之後有一個 [略過] 連結，您可以在確定不要修復此問題的時候，選擇略過。如果您之後決定要修復上次略過的問題，可將問題併入保護狀態中以進行追蹤。

若要設定略過的問題：

1 在 [SecurityCenter 資訊] 底下按一下 [設定]。
2 按一下 [保護狀態] 旁的箭號以展開窗格，然後按一下 [進階]。
3 在 [略過的問題] 窗格中執行下列其中一項動作：
   - 若要將先前略過的問題併入保護狀態中，請清除其核取方塊。
   - 若要將問題排除於保護狀態之外，請選擇其核取方塊。
4 按一下 [確定]。

設定使用者選項

如果您正在執行需要使用者權限的 McAfee 程式，則根據預設這些權限會對應至您電腦的 Windows 使用者帳戶。若要更輕易地管理這些程式的使用者，您可隨時切換到使用 McAfee 使用者帳戶。

若您切換爲使用 McAfee 使用者帳戶，會自動匯入任何現有的未成年保護程式使用者名稱及權限。然而首次切換時，您必須建立一個管理員帳戶。之後就可以開始建立並設定其他 McAfee 使用者帳戶。

切換爲 McAfee 使用者帳戶

依預設您會使用 Windows 使用者帳戶。然而，切換爲 McAfee 使用者帳戶就不用建立額外的 Windows 使用者帳戶了。

若要切換爲 McAfee 使用者帳戶：

1 在 [SecurityCenter 資訊] 底下按一下 [設定]。

2 按一下 [使用者] 旁的箭號以展開窗格，然後按一下 [進階]。

3 若要使用 McAfee 使用者帳戶，按一下 [切換]。

如果是首次切換爲 McAfee 使用者帳戶，您必須建立管理員帳戶 (第 25 頁)。

建立管理員帳戶

首次切換爲使用 McAfee 使用者時，系統會提示您建立管理員帳戶。

若要建立管理員帳戶：

1 在 [密碼] 方塊中輸入密碼，然後在 [確認密碼] 方塊中重新輸入一次。

2 在清單中選擇密碼回復問題，然後在 [答案] 方塊中輸入秘密問題的答案。

3 按一下 [套用]。

   完成後，未成年保護程式中若有現有的使用者名稱及權限，就會使用它們來更新窗格中的使用者帳戶類型。若是首次設定使用者帳戶，會出現 [管理使用者] 窗格。

設定使用者選項

若您切換爲使用 McAfee 使用者帳戶，會自動匯入任何現有的未成年保護程式使用者名稱及權限。然而首次切換時，您必須建立一個 Administrator 帳戶。之後就可以開始建立並設定其他 McAfee 使用者帳戶。

若要設定使用者選項：

1 在 [SecurityCenter 資訊] 底下按一下 [設定]。

2 按一下 [使用者] 旁的箭號以展開窗格，然後按一下 [進階]。

3 在 [使用者帳戶] 下按一下 [新增]。

4 在 [使用者名稱] 方塊中輸入使用者名稱。

5 在 [密碼] 方塊中輸入密碼，然後在 [確認密碼] 方塊中重新輸入一次。

6 若您要讓這位新使用者在 SecurityCenter 啓動時自動登入，請選擇 [啓動使用者] 核取方塊。

7 在 [使用者帳戶類型] 下選擇此使用者的帳戶類型，再按一下 [建立]。

注意：建立使用者帳戶後，必須在 [未成年保護] 下設定 [受限的使用者] 的設定。

8 若要編輯使用者密碼、自動登入或帳戶類型，請在清單中選擇使用者名稱，再按一下 [編輯]。

9 完成後，按一下 [套用]。

擷取管理員密碼

如果您忘記管理員密碼，可擷取該密碼。

若要擷取管理員密碼：

1 以滑鼠右鍵按一下 SecurityCenter M 圖示 ，然後按一下 [切換使用者]。

2 在 [使用者名稱] 清單中選擇 [管理員]，然後按一下 [忘記密碼了嗎]。

3 輸入您在建立管理員帳戶時選擇的秘密問題答案。

4 按一下 [提交]。

隨即出現您忘記的管理員密碼。

變更管理員密碼

若您不記得管理員密碼或懷疑密碼遭到洩漏，您可以變更密碼。

若要變更管理員密碼：

1 以滑鼠右鍵按一下 SecurityCenter M 圖示，然後按一下 [切換使用者]。
2 在 [使用者名稱] 清單中選擇 [管理員]，然後按一下 [變更密碼]。
3 在 [舊密碼] 方塊中輸入您現有的密碼。
4 在 [密碼] 方塊中輸入新密碼，然後在 [確認密碼] 方塊中重新輸入一次。
5 按一下 [確定]。

設定更新選項

當您連線到網際網路時，SecurityCenter 每隔四個小時便會自動檢查所有的 McAfee 服務是否已更新，然後自動安裝最新的產品更新。然而，您隨時可使用工作列最右邊通知區域中的 SecurityCenter 圖示，手動檢查更新。

自動檢查更新

當您連線到網際網路時，SecurityCenter 每隔四個小時便會自動檢查一次更新。然而您可設定 SecurityCenter，使其在下載或安裝更新前通知您。

若要自動檢查更新：

1. 在 [SecurityCenter 資訊] 底下按一下 [設定]。
2. 按一下 [自動更新已啟用] 狀態旁的箭號以展開窗格，然後按一下 [進階]。
3. 在 [更新選項] 窗格中選擇下列其中一個選項：
   - 自動安裝更新並在產品更新後通知我 (建議使用) (第 29 頁)
   - 自動下載更新並在可以安裝時通知我 (第 29 頁)
   - 在下載任何更新之前通知我 (第 30 頁)
4. 按一下 [確定]。

注意：McAfee 建議您讓 SecurityCenter 自動檢查並安裝更新，以達到最佳保護效果。然而，如果只要手動更新安全服務，您可以停用自動更新 (第 30 頁)。

自動下載並安裝更新

如果您選擇 [SecurityCenter 更新選項] 中的 [自動安裝更新並在服務更新後通知我 (建議使用)]，SecurityCenter 便會自動下載並安裝更新。

自動下載更新

如果您選擇 [更新選項] 中的 [自動下載更新並在可以安裝時通知我]，SecurityCenter 便會自動下載更新，並在可以安裝更新時通知您。然後，您可以選擇安裝更新或延期更新 (第 30 頁)。

若要自動安裝已下載的更新：

1. 在警示上按一下 [立即更新產品]，然後按一下 [確定]。

   如果出現提示要求您登入網站，則必須登入以確認訂閱，然後才能進行下載。

2. 確認訂閱之後，請於 [更新] 窗格上按一下 [更新]，下載並安裝更新。如果您的訂閱已經到期，按一下警示上的 [續訂] 並遵循提示進行。

注意：在某些情況中，您會看到提示要求您重新啟動電腦，以便完成更新。請儲存所有工作並關閉所有程式之後，再重新啟動。

在下載更新前通知您

如果您選擇 [更新選項] 窗格中的 [在下載任何更新之前通知我]，SecurityCenter 便會在下載任何更新前通知您。然後，您便可以選擇下載並安裝安全服務的更新，以消除攻擊的威脅。

若要下載並安裝更新：

1 在警示上選擇 [立即更新產品]，然後按一下 [確定]。
2 如果出現提示，請登入網站。

 便會自動下載更新。

3 更新安裝完成後，按一下警示上的 [確定]。

> **注意：**在某些情況中，您會看到提示要求您重新啓動電腦，以便完成更新。請儲存所有工作並關閉所有程式之後，再重新啓動。

停用自動更新

McAfee 建議您讓 SecurityCenter 自動檢查並安裝更新，以達到最佳保護效果。然而，如果只要手動更新安全性服務，您可以停用自動更新。

> **注意：**請一定要記住，每週至少要手動檢查更新 (第 31 頁) 一次。如果沒有檢查更新，電腦將無法得到最新安全性更新所提供的保護。

若要停用自動更新：

1 在 [SecurityCenter 資訊] 底下，按一下 [設定]。
2 按一下 [自動更新已啓用] 狀態旁的箭號以展開窗格。
3 按一下 [關閉]。
4 按一下 [是] 確認變更。

 狀態會在標頭中更新。

如果七天內未手動檢查更新，會有警示提醒您檢查更新。

延期更新

如果您太忙，無法在出現警示時更新您的安全服務，則可以選擇稍後再提醒或略過警示。

若要延期更新：

- 執行下列其中一項：
  - 在警示上選擇 [稍後提醒我]，然後按一下 [確定]。
  - 選擇 [關閉此警示]，再按一下 [確定]，關閉警示且不採取任何動作。

手動檢查更新

當您連線到網際網路時，SecurityCenter 每隔四個小時便會自動檢查一次更新，然後會安裝最新的產品更新。然而，您隨時可使用工作列最右邊 Windows 通知區域中的 SecurityCenter 圖示，手動檢查更新。

注意：McAfee 建議您讓 SecurityCenter 自動檢查並安裝更新，以達到最佳保護效果。然而，如果只要手動更新安全服務，您可以停用自動更新 (第 30 頁)。

若要手動檢查更新：

1 請確定您的電腦已與網際網路連線。

2 在工作列最右邊的 Windows 通知區域中的 SecurityCenter M 圖示 上按一下滑鼠右鍵，再按一下 [更新]。

   您可以在 SecurityCenter 檢查是否有更新時，繼續執行其他相關工作。

   工作列最右邊的 Windows 通知區域會顯示一個動畫圖示，方便您參考。SecurityCenter 完成之後，圖示會自動消失。

3 如果出現提示，請登入網站以驗證訂閱。

注意：在某些情況中，您會看到提示要求您重新啟動電腦，以便完成更新。請儲存所有工作並關閉所有程式之後，再重新啟動。

設定警示選項

SecurityCenter 會透過警示與聲音，自動通知您大範圍的病毒爆發、安全性威脅及產品更新。然而，您可以設定 SecurityCenter 僅顯示需要您立即注意的警示。

設定警示選項

SecurityCenter 會透過警示與聲音，自動通知您公開的病毒爆發、安全性威脅及產品更新。但您可以設定 SecurityCenter 僅顯示需要您立即注意的警示。

若要設定警示選項：

1 在 [SecurityCenter 資訊] 底下按一下 [設定]。

2 按一下 [警示] 旁的箭號以展開窗格，然後按一下 [進階]。

3 在 [警示選項] 窗格中選擇下列其中一項：

- **當公開的病毒爆發或安全性威脅發生時，請發出警示**
- **偵測到遊戲模式時，顯示資訊警示**
- **出現警示時播放聲音**
- **Windows 啓動時顯示 McAfee 片頭畫面**

4 按一下 [確定]。

注意：若要從警示本身停用日後的資訊警示，請選擇 [不要再顯示此警示] 核取方塊。之後您可在 [資訊警示] 窗格中再次啓用。

設定資訊警示

資訊警示會在發生不需立即回應的事件時進行通知。若從警示本身停用日後的資訊警示，以後您可在 [資訊警示] 窗格中再次啓用。

若要設定資訊警示：

1 在 [SecurityCenter 資訊] 底下，按一下 [設定]。

2 按一下 [警示] 旁的箭號以展開窗格，然後按一下 [進階]。

3 在 [SecurityCenter 設定] 底下，按一下 [資訊警示]。

4 清除 [隱藏資訊警示] 核取方塊，然後清除清單中您想顯示之警示的核取方塊。

5 按一下 [確定]。

第 5 章

執行常見工作

您可執行的常見工作包含回到 [首頁] 窗格、檢視最近的事件、管理電腦網路 (如果您位於具有此網路之管理功能的電腦上)，以及維護電腦。如果已安裝 McAfee Data Backup，您還可以備份資料。

在本章中

執行常見工作

您可執行的常見工作包含回到 [首頁] 窗格、檢視最近的事件、維護電腦、管理電腦網路 (如果您位於具有此網路之管理功能的電腦上)，以及備份資料 (如果已安裝 McAfee Data Backup)。

若要執行常見工作：

- 在 [基本功能表] 中的 [常見工作] 下，執行下列其中一項動作：
  - 若要回到 [首頁] 窗格，請按一下 [首頁]。
  - 若要檢視安全性軟體偵測到的最近事件，按一下 [檢視最近的事件]。
  - 若要移除不使用的檔案、重組資料並將電腦還原為先前的設定，按一下 [維護電腦]。
  - 若要管理電腦網路，在具有網路管理能力的電腦上按一下 [管理網路]。

    Network Manager 會監視網路上各電腦的安全弱點，讓您輕鬆識別網路安全性問題。
  - 若要建立檔案的備份複本，按一下 [Data Backup] (若已安裝 McAfee Data Backup)。

    自動備份可視您的需要儲存您最珍檔案的副本，在 CD/DVD、USB、外部或網路磁碟機上加密並儲存您的檔案。

秘訣：為了方便使用，您可從兩個額外的位置執行常見工作 ([進階功能表] 中的 [首頁]，及工作列最右邊 SecurityCenter M 圖示的 [快速連結] 功能表)。您也可以在 [進階功能表] 上的 [報告與記錄] 下，依照類型檢視最近的事件及詳細的記錄。

檢視最近的事件

當電腦發生變更時便會記錄最近的事件。這些變更的範例包括：啓用或停用保護類型時、移除威脅時，或封鎖網際網路連線嘗試時。您可檢視 20 筆最近的事件及其詳細資料。

如需事件的詳細資料，請參閱相關產品的說明檔。

若要檢視最近的事件：

1 在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，然後按一下 [檢視最近的事件]。

   任何在清單中出現的最近事件都會顯示日期及簡短描述。

2 在 [最近的事件] 下選擇事件，便能在 [詳細資料] 窗格中檢視額外的資訊。

   在 [我想要] 下會出現所有可採取的動作。

3 若要檢視更詳細的事件清單，按一下 [檢視記錄檔]。

自動維護電腦

若要釋放珍貴的磁碟空間並最佳化電腦效能，您可排定時間，讓 QuickClean 或磁碟重組工具定期執行工作。這些工作包含刪除、壓縮及重組檔案及資料夾。

若要自動維護電腦：

1 在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，然後按一下 [維護電腦]。

2 在 [工作排程器] 下按一下 [開始]。

3 在操作清單中，選擇 [QuickClean] 或 [磁碟重組工具]。

4 執行下列其中一項：

   - 若要修改現有的工作，請選擇工作然後按一下 [修改]。遵循螢幕上的指示進行。
   - 若要建立新工作，請在 [工作名稱] 方塊中輸入名稱，然後按一下 [建立]。遵循螢幕上的指示進行。
   - 若要刪除現有的工作，請選擇工作然後按一下 [刪除]。

5 在 [工作摘要] 下檢視上次執行工作的時間、下次執行的時間及狀態。

手動維護電腦

您可以手動執行維護工作來移除不使用的檔案、重組資料或將電腦還原為先前的設定。

若要手動維護電腦：

- 執行下列其中一項：
  - 若要使用 QuickClean，在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，再按一下 [維護電腦]，然後按一下 [開始]。
  - 若要使用 [磁碟重組工具]，在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，再按一下 [維護電腦]，然後按一下 [分析]。
  - 若要使用 [系統還原]，在 [進階功能表] 上依序按一下 [工具]、[系統還原] 及 [開始]。

移除不使用的檔案及資料夾

使用 QuickClean 釋放珍貴的磁碟空間並最佳化電腦效能。

若要移除不使用的檔案及資料夾：

1. 在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，然後按一下 [維護電腦]。
2. 在 [QuickClean] 下按一下 [開始]。
3. 遵循螢幕上的指示進行。

重組檔案與資料夾

在刪除檔案及資料夾並新增檔案時，會發生檔案分散的情形。檔案分散會減慢磁碟存取的速度並降低電腦的整體效能 (雖然影響程度並不大)。

使用磁碟重組將檔案部份重新寫入到硬碟上的連續磁區，以增加存取及擷取的速度。

若要重組檔案與資料夾：

1. 在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，然後按一下 [維護電腦]。
2. 在 [磁碟重組工具] 底下按一下 [分析]。
3. 遵循螢幕上的指示進行。

將電腦還原爲先前的設定

還原點即爲 Windows 在發生重要事件時 (如安裝程式或驅動程式時)，以及定期儲存的電腦快照。然而，您可隨時建立並命名自己的還原點。

使用還原點，可以復原對電腦的有害變更，並回到先前的設定。

若要將電腦還原爲先前的設定：

1 在 [進階功能表] 上，按一下 [工具]，然後按一下 [系統還原]。

2 在 [系統還原] 下按一下 [開始]。

3 遵循螢幕上的指示進行。

管理網路

如果電腦具有網路的管理功能，您便能使用 Network Manager 來監視網路上的電腦是否有安全弱點，讓您輕鬆識別安全性問題。

如果電腦的保護狀態在此網路上未受到監視，則電腦若不是此網路的成員，就是此網路未管理的成員。如需詳細資料，請參閱 Network Manager 說明檔。

若要管理網路：

1 在主要 SecurityCenter 圖示上按滑鼠右鍵，並指向 [快速連結]，然後按一下 [管理網路]。

2 在網路圖上按一下代表此電腦的圖示。

3 在 [我想要] 下按一下 [監視此電腦]。

深入瞭解病毒

使用病毒資訊庫及病毒活動圖來進行下列動作：

- 深入瞭解最新型的病毒、電子郵件病毒惡作劇，以及其他威脅。
- 取得免費的病毒移除工具，以協助您修復電腦。
- 即時瞭解全球何處正遭受最新電腦病毒的侵襲。

若要深入瞭解病毒：

1 在 [進階功能表] 上，按一下 [工具]，然後按一下 [病毒資訊]。

2 執行下列其中一項：

   - 使用免費的 McAfee 病毒資訊庫來研究病毒。
   - 使用 McAfee 網站中的 World Virus Map 來研究病毒。

第　6　章

McAfee QuickClean

您瀏覽網際網路時，電腦上很快會累積零亂的檔案。請使用 QuickClean 來保護您的隱私，並刪除不需要的網際網路和電子郵件零亂檔案。QuickClean 會識別及刪除瀏覽時累積的檔案，包括 Cookie、電子郵件、下載及歷史記錄 (即包含您個人資訊的資料)。它能夠安全地刪除此一機密資訊，以保護您的隱私。

QuickClean 也可以刪除無用的程式。指定您要消除的檔案，然後在不刪除必要資訊的前提下消除零亂的檔案。

在本章中

瞭解 QuickClean 功能

本節說明 QuickClean 功能。

功能

QuickClean 提供一組有效且易於使用的工具，讓您安全地刪除數位碎片。您可以釋出珍貴的磁碟機空間，並最佳化您的電腦效能。

第 7 章

清理您的電腦

QuickClean 可讓您安全地刪除檔案及資料夾。

當您瀏覽網際網路時，瀏覽器會將每一個網頁及其圖形複製到您磁碟上的快取資料夾。如果您再次返回網頁，瀏覽器就能迅速地載入該頁面。如果您重複地造訪相同的網頁，而且其內容不常變更，則快取檔案很有用。然而，大多情形下，快取的檔案並不實用，因此能夠加以刪除。

您可以利用下列清理工具來刪除各種項目。

- 資源回收筒清理工具：清理您的 Windows [資源回收筒]。
- 暫存檔清理工具：刪除暫存資料夾中儲存的檔案。
- 捷徑清理工具：刪除中斷的捷徑及沒有關聯程式的捷徑。
- 遺失的檔案片段清理工具：從您的電腦中刪除遺失的檔案片段。
- 登錄清理工具：刪除電腦中已不存在之程式的 Windows 登錄資訊。
- 快取清理工具：刪除您在瀏覽網際網路時累積的快取檔案。這種類型的檔案通常會儲存為網際網路暫存檔。
- Cookie 清理工具：刪除 Cookie。這種類型的檔案通常會儲存為網際網路暫存檔。
  Cookie 為 Web 瀏覽器應 Web 伺服器要求，而儲存於您電腦上的小型檔案。您每次從 Web 伺服器檢視網頁時，瀏覽器就會將 Cookie 送回伺服器。這些 Cookie 的功用就像標籤，讓 Web 伺服器追蹤您檢視的網頁，以及您返回那些網頁頻繁的程度。
- 瀏覽器歷史記錄清理工具：刪除您的瀏覽器歷史記錄。
- 用來清理已刪除及已傳送項目的 Outlook Express 及 Outlook 電子郵件清理工具：從 Outlook [寄件匣] 及 [刪除的郵件] 資料夾中刪除郵件。
- 最近使用過項目的清理工具：刪除儲存在電腦上，您最近使用過的項目，例如 Microsoft Office 文件。
- ActiveX 與 Plug-in 清理工具：刪除 ActiveX 控制項與 Plug-in。
  ActiveX 是一種用來執行程式中控制項的技術。ActiveX 控制項可將按鈕新增至程式的介面。這些控制項大部份都是無害的；然而，有些人會使用 ActiveX 技術來擷取您電腦中的資訊。
  Plug-in (外掛程式) 為插到大型應用程式以提供附加功能的小型軟體程式。Plug-in 會允許 Web 瀏覽器存取並執行 HTML 文件中內含的檔案，瀏覽器通常無法辨識這些檔案的格式 (例如，動畫檔、視訊檔及音效檔)。

- 系統還原點清理工具：從您的電腦刪除舊的系統還原點。

在本章中

使用 QuickClean

本節說明 QuickClean 的使用方法。

清理您的電腦

您可以刪除未使用的檔案及資料夾，釋出磁碟空間，讓電腦的執行更有效率。

清理電腦：

1. 在 [進階功能表] 上，按一下 [工具]。
2. 按一下 [維護電腦]，然後按一下 [McAfee QuickClean] 底下的 [開始]。
3. 執行下列其中一項：
   - 按 [下一步] 以接受清單中的預設清理工具。
   - 選擇或清除適合的清理工具，然後按 [下一步]。若為最近使用過項目的清理工具，您可以按一下 [內容]，清除您不想要清理其清單的程式。
   - 按一下 [還原預設值]，還原預設清理工具，再按 [下一步]。
4. 執行分析之後，請按 [下一步] 以確認刪除檔案。您可以展開此清單，以查看即將清理的檔案及其位置。
5. 按 [下一步]。
6. 執行下列其中一項：
   - 按 [下一步] 以接受預設的 [否，我要使用標準 Windows 刪除作業來刪除檔案]。
   - 按一下 [是，我要使用 Shredder 安全地清除檔案]，並指定操作數目。利用 Shredder 刪除的檔案將無法回復。
7. 按一下 [完成]。
8. 在 [QuickClean 摘要] 底下，檢視已刪除的登錄檔數目，以及在清理磁碟及網際網路之後收回的磁碟空間數量。

第 8 章

McAfee Shredder

即使您清空資源回收筒之後，仍然可以從您的電腦復原刪除的檔案。您刪除檔案時，Windows 會將您磁碟機上的該空間標示為不再使用，但是檔案仍在該處。使用電腦分析工具，可以還原稅務記錄、工作履歷表，或您已刪除的其他文件。Shredder 會安全且永久地刪除無用的檔案，以保護您的隱私。

若要永久刪除檔案，必須在現有檔案上重複覆寫新資料。Microsoft® Windows 不會安全地刪除檔案，因為每個檔案作業會很慢。將文件銷毀不一定能防止文件被復原，因為有些程式會儲存開啓之文件的暫存隱藏副本。如果您只銷毀在 Windows® 檔案總管裡看到的文件，這些文件還是可能有暫存副本。

注意： 銷毀的檔案不會備份。Shredder 已刪除的檔案無法再還原。

在本章中

瞭解 Shredder 功能

本節說明 Shredder 功能。

功能

Shredder 能讓您清除 [資源回收筒] 內容、網際網路暫存檔、網站歷史記錄、檔案、資料夾及磁碟。

第　9　章

利用 Shredder 清除無用檔案

Shredder 可以安全地並永久地刪除無用檔案 (例如,[資源回收筒] 內容、網際網路暫存檔及網站歷史記錄) 來保護您的隱私。您可以選擇要銷毀的檔案及資料夾，或以瀏覽方式加以尋找。

在本章中

使用 Shredder

本節說明 Shredder 的使用方法。

銷毀檔案、資料夾及磁碟

即使您已清空 [資源回收筒]，檔案仍可能存在於您的電腦中。然而，檔案一經銷毀，就會永久地刪除資料，駭客便無法予以存取。

銷毀檔案、資料夾及磁碟：

1 在 [進階功能表] 上，按一下 [工具]，然後按一下 [Shredder]。
2 執行下列其中一項：
   - 按一下 [清除檔案與資料夾] 來銷毀檔案與資料夾。
   - 按一下 [清除整個磁碟] 來銷毀磁碟。
3 選擇下列其中一個銷毀層級：
   - 快速：銷毀所選項目一次。
   - 全面：銷毀所選項目七次。
   - 自訂：銷毀所選項目，最多十次。銷毀操作的次數越高，安全刪除檔案的層級就越高。
4 按 [下一步]。
5 執行下列其中一項：
   - 如果您要銷毀檔案，請在 [選擇要銷毀的檔案] 清單中，按一下 [資源回收筒內容]、[Temporary Internet files] 或 [網站歷史記錄]。如果要銷毀磁碟，請按一下磁碟。
   - 按一下 [瀏覽]，瀏覽至您要銷毀的檔案，然後加以選取。
   - 在 [選擇要銷毀的檔案] 清單中，鍵入您要銷毀之檔案的路徑。
6 按 [下一步]。
7 按一下 [完成] 以完成作業。
8 按一下 [完成]。

第　10　章

McAfee Network Manager

McAfee® Network Manager 展現了組成家庭網路之電腦與元件的圖形化檢視畫面。您可以使用 Network Manager，從遠端監視您網路上每台受管理電腦的保護狀態，並在遠端修復這些受管理電腦上所報告的安全性弱點。

開始使用 Network Manager 之前，請先熟悉一些最常用的功能。Network Manager 說明中會提供有關設定和使用這些功能的詳細資料。

在本章中

功能

Network Manager 提供了下列功能：

圖形化網路圖

Network Manager 的網路圖提供組成家庭網路之電腦與元件的安全性狀態圖形化總覽。當您對網路進行變更時 (例如，增加一部電腦)，網路圖會識別這些變更。您可以重新整理網路圖、重新命名網路、顯示或隱藏網路圖元件以自訂您的檢視畫面。您也可以檢視與網路圖上任何顯示元件相關的詳細資料。

遠端管理

使用 Network Manager 網路圖來管理組成您家庭網路之電腦的安全性狀態。您可邀請電腦加入受管理網路、監視受管理電腦的保護狀態，並從網路上的遠端電腦修正已知安全性弱點。

瞭解 Network Manager 圖示

下表說明 Network Manager 網路圖上常用的圖示。

圖示	說明
	表示一個線上受管理的電腦
	表示一個離線受管理的電腦
	表示一個安裝了 McAfee 2007 安全性軟體的不受管理電腦
	表示一個離線不受管理的電腦
	表示一個未安裝 McAfee 2007 安全性軟體的線上電腦，或一個未知的網路裝置
	表示一個未安裝 McAfee 2007 安全性軟體的離線電腦，或一個離線未知的網路裝置
	意味著對應的項目受到保護並已連線
	意味著對應的項目需要您的注意
	意味著對應的項目需要您的注意，並已中斷連線
	表示無線家用路由器
	表示一個標準的家用路由器
	表示連線時的網際網路
	表示中斷連線時的網際網路

第 11 章

設定一個受管理網路

透過與您網路圖上的項目一起運作及新增網路成員 (電腦) 至網路來設定一個受管理網路。

在本章中

與網路圖一起運作

您每次將電腦連線至網路時，Network Manager 會分析網路狀態以決定是否有任何成員 (受管理與不受管理) 存在、路由器的屬性及網際網路狀態。若未發現任何成員，Network Manager 會假設目前連線的電腦是網路上第一台電腦，並自動使該台電腦成爲具管理權限的受管理成員。依預設，網路名稱包含首部連線至安裝 McAfee 2007 安全性軟體網路之電腦所在工作群組或網域的名稱；然而，您可隨時重新命名網路。

當您對網路進行變更時 (例如，增加一部電腦)，您可自訂網路圖。例如，您可以重新整理網路圖、重新命名網路，顯示或隱藏網路圖元件以自訂您的檢視畫面。您也可以檢視與網路圖上任何顯示元件相關的詳細資料。

存取網路圖

從常見工作的 SecurityCenter 清單啓動 Network Manager 來存取您的網路圖。網路圖提供了組成家庭網路之電腦與元件的圖形化呈現。

若要存取網路圖：

- 在 [基本功能表] 或 [進階功能表] 上，按一下 [管理網路]。
  網路圖便會顯示於右窗格中。

注意：您第一次存取網路圖時，系統會在顯示網路圖之前，提示您信任網路上的其他電腦。

重新整理網路圖

您可隨時重新整理網路圖；例如，於另一個電腦加入受管理網路後。

若要重新整理網路圖：

1 在 [基本功能表] 或 [進階功能表] 上，按一下 [管理網路]。
  網路圖便會顯示於右窗格中。
2 按一下 [我要] 下的 [重新整理網路圖]。

注意：[重新整理網路圖] 連結僅適用於未在網路圖上選取任何項目時。若要取消選取一個項目，請按一下所選取的項目，或按一下網路圖上的空白區域。

重新命名網路

依預設，網路名稱包含首部連線至安裝 McAfee 2007 安全性軟體網路之電腦所在工作群組或網域的名稱。若名稱不恰當，您可以變更。

若要重新命名網路：

1. 在 [基本功能表] 或 [進階功能表] 上，按一下 [管理網路]。網路圖便會顯示於右窗格中。
2. 按一下 [我要] 下的 [重新命名網路]。
3. 於 [重新命名網路] 方塊中鍵入網路名稱。
4. 按一下 [確定]。

注意：[重新命名網路] 連結僅適用於未在網路圖上選取任何項目時。若要取消選取一個項目，請按一下所選取的項目，或按一下網路圖上的空白區域。

顯示或隱藏網路圖上的項目

依預設，您家庭網路中的所有電腦與元件都會顯示在網路圖上。然而，若您有隱藏的項目，您可隨時再次顯示他們。只有不受管理的項目可以隱藏；受管理的電腦不能隱藏。

若要...	在 [基本功能表] 或 [進階功能表] 上，按一下 [管理網路]，然後執行...
隱藏網路圖上的項目	按一下網路圖上的項目，然後按一下 [我要] 下的 [隱藏此項目]。於確認對話方塊中，按一下 [是]。
顯示網路圖上隱藏的項目	在 [我要] 下，按一下 [顯示隱藏的項目]。

檢視項目的詳細資料

您可以選取網路圖上的元件，檢視您網路上有關該元件的詳細資訊。此資訊包括元件名稱、元件保護狀態，及管理元件所需要的其他資訊。

若要檢視項目的詳細資料：

1 按一下網路圖上的項目圖示。

2 在 [詳細資料] 下，檢視有關項目的資訊。

加入受管理網路

一部電腦必須先成爲網路的信任成員，才能對該電腦進行遠端管理，或授予其遠端管理網路上其他電腦的權限。新電腦的網路成員資格是由具管理權限的現有網路成員 (電腦) 所授予。爲確保只有信任的電腦才可加入網路，授權電腦及加入電腦雙方的使用者必須驗證彼此。

當一部電腦加入網路時，會出現提示要求它對網路上其他電腦顯示其 McAfee 保護狀態。若某部電腦同意顯示其保護狀態，它即會成爲網路的受管理成員。某部電腦若拒絕顯示其保護狀態，它即會成爲網路的不受管理成員。網路的不受管理成員通常是要存取其他網路功能 (例如，檔案或印表機共用) 的來賓電腦。

注意：加入後，若您已安裝了其他 McAfee 網路程式 (例如，McAfee Wireless Network Security 或 EasyNetwork)，則該電腦仍爲這些程式視爲一個受管理的電腦。指定給 Network Manager 中之電腦的權限等級會套用至所有 McAfee 網路程式。針對來賓權限、完整權限或系統管理權限在其他 McAfee 網路程式中的意義，請參閱該程式所提供的說明文件，以取得詳細資訊。

加入受管理網路

當您收到加入受管理網路的邀請時，您可以接受或拒絕邀請。您亦可決定是否要讓此電腦與網路上其他電腦互相監視彼此的安全性設定 (例如，電腦的病毒保護是否是最新的)。

若要加入受管理網路：

1. 在邀請對話方塊中，請啓用 [允許此電腦和其他電腦監視彼此的安全性設定] 核取方塊，讓受管理網路上的其他電腦監視您電腦的安全性設定。
2. 按一下 [加入]。
   當您接受邀請時，即會顯示兩種圖片。
3. 請確認該圖片與邀請您加入受管理網路之電腦上所顯示的圖片相同。
4. 按一下 [確認]。

注意：若邀請您加入受管理網路的電腦並未顯示相同的圖片 (其顯示於安全性確認對話方塊中)，則表示受管理網路上發生安全漏洞。加入網路可能會讓您的電腦面臨風險，因此，請按一下安全性確認對話方塊中的 [拒絕]。

邀請電腦加入受管理網路

若某部電腦新增至受管理網路或其他存在於網路中的不受管理電腦，則您可邀請該電腦加入受管理網路。只有在網路上具管理權限的電腦可以邀請其他電腦加入網路。當您傳送邀請時，您也需要對加入的電腦指定您要指派的權限等級。

若要邀請電腦加入受管理網路：

1 按一下網路圖上的不受管理電腦圖示。
2 按一下 [我要] 下的 [監視此電腦]。
3 於 [邀請電腦加入受管理網路] 對話方塊中，按一下下列其中一項：
   - **授予來賓存取權**
     來賓存取權可讓電腦存取網路。
   - **對所有受管理網路應用程式授予完整存取權**
     完整存取權 (就像來賓存取權一樣) 可讓電腦存取網路。
   - **對所有受管理網路應用程式授予管理存取權**
     管理存取權可讓電腦以管理權限存取網路。其亦可讓電腦對要加入受管理網路的其他電腦授予存取權。
4 按一下 [邀請]。
   加入受管理網路的邀請會傳送至該電腦。當電腦接受邀請時，即會顯示兩種圖片。
5 請確認該圖片與您已邀請加入受管理網路之電腦上所顯示的圖片相同。
6 按一下 [授予存取權]。

注意：若您邀請加入受管理網路的電腦並未顯示相同的圖片 (其顯示於安全性確認對話方塊中)，則表示受管理網路上發生安全漏洞。允許電腦加入網路可能導致其他電腦處於風險之中，因此，按一下安全性確認對話方塊中的 [拒絕存取權]。

停止信任網路上的電腦

如果您錯誤地同意信任網路上的其他電腦，您可以停止信任他們。

若要停止信任網路上的電腦：

- 按一下 [我要] 下的 [停止信任此網路上的電腦]。

注意：當沒有其他受管理電腦加入網路時，才能使用 [停止信任此網路上的電腦] 連結。

第　12　章

遠端管理網路

設定您的受管理網路後，您可使用 Network Manager 在遠端管理組成您網路的電腦與元件。您可以監視電腦與元件的狀態及權限等級並從遠端修復安全性弱點。

在本章中

監視狀態與權限

受管理網路具有兩種成員類型：受管理成員與不受管理成員。受管理成員可讓網路上其他電腦監視其 McAfee 保護狀態；而不受管理成員則否。不受管理成員通常是要存取其他網路功能 (例如，檔案或印表機共用) 的來賓電腦。不受管理電腦可隨時爲網路上其他受管理電腦所邀請，成爲一部受管理電腦。同樣的，受管理電腦可隨時成爲不受管理電腦。

受管理電腦具有與他們相關聯的管理權限，完整權限或來賓權限。管理權限可讓受管理電腦管理網路上所有其他受管理電腦的保護狀態，並對其他電腦授予網路的成員資格。完整權限與來賓權限只允許一部電腦存取網路。您可隨時修改電腦的權限等級。

因爲受管理網路亦包含了裝置 (例如，路由器)，您也可以使用 Network Manager 來管理這些裝置。您還可以設定並修改網路圖上之裝置的顯示內容。

監視電腦的保護狀態

如果電腦的保護狀態在此網路上未受到監視 (因爲該電腦不是該網路的成員，或該電腦是該網路的不受管理成員)，則您可提出對其進行監視的要求。

若要監視電腦的保護狀態：

1 按一下網路圖上的不受管理電腦圖示。
2 按一下 [我要] 下的 [監視此電腦]。

停止監視電腦的保護狀態

您可以停止監視您私人網路中受管理電腦的保護狀態。之後，此電腦會成爲一部不受管理的電腦。

若要停止監視電腦的保護狀態：

1 按一下網路圖上的受管理電腦圖示。
2 按一下 [我要] 下的 [停止監視此電腦]。
3 於確認對話方塊中，按一下 [是]。

修改受管理電腦的權限

您可隨時修改受管理電腦的權限。這能讓您調整哪部電腦可監視網路上其他電腦的保護狀態 (安全性設定)。

若要修改受管理電腦的權限：

1. 按一下網路圖上的受管理電腦圖示。
2. 按一下 [我要] 下的 [修改此電腦的權限]。
3. 在修改權限對話方塊中，請選取或清除核取方塊，以決定此電腦及受管理網路上的其他電腦是否可以監視彼此的保護狀態。
4. 按一下 [確定]。

管理裝置

您可由 Network Manager 內存取其管理網頁來管理裝置。

若要管理裝置：

1. 按一下網路圖上的裝置圖示。
2. 按一下 [我要] 下的 [管理此裝置]。
   Web 瀏覽器將會開啓並顯示裝置的管理網頁。
3. 在您的 Web 瀏覽器中，請提供您的登入資訊並設定裝置的安全性設定。

注意：若該裝置是一個 Wireless Network Security 保護的無線路由器或存取點，您必須使用 Wireless Network Security 來進行該裝置的安全性設定。

修改裝置的顯示內容

修改裝置顯示內容時，您可以變更網路圖上的裝置顯示名稱，並指定裝置是否為一個無線路由器。

若要修改裝置的顯示內容：

1. 按一下網路圖上的裝置圖示。
2. 按一下 [我要] 下的 [修改裝置內容]。
3. 若要指定裝置的顯示名稱，請於 [名稱] 方塊中鍵入名稱。
4. 若要指定裝置類型，請按下列其中一項：
   - **路由器**
     此表示一個標準的家用路由器。
   - **無線路由器**
     此表示一個無線家用路由器。

5 按一下 [確定]。

修復安全性弱點

具管理權限的受管理電腦可以監視網路上其他受管理電腦的 McAfee 保護狀態，並從遠端修復任何回報的安全性弱點。例如，若一部受管理電腦的 McAfee 保護狀態指出其 VirusScan 已停用，則另一個具管理權限的受管理電腦可從遠端啓用 VirusScan 來修復此安全性弱點。

當您從遠端修復安全性弱點時，Network Manager 會自動修復最常報告的問題。然而，某些安全性弱點可能需要在本機電腦上手動介入。在這種情況下，Network Manager 會修復那些可遠端修復的問題，然後提示您登入易受入侵之電腦的 SecurityCenter 中，並遵循所提供的建議修復剩下的問題。在某些情況下，建議的修復措施是在遠端或您網路中的電腦上安裝 McAfee 2007 安全性軟體。

修復安全性弱點

您可使用 Network Manager，自動修復遠端受管理電腦上的大部分安全性弱點。例如，若在一個遠端電腦上已停用了 VirusScan，則您可使用 Network Manager 來自動啓用它。

若要修復安全性弱點：

1. 按一下網路圖上的項目圖示。
2. 檢視 [詳細資料] 下之項目的保護狀態。
3. 按一下 [我要] 下的 [修復安全性弱點]。
4. 當安全性問題修復之後，請按一下 [確定]。

注意：雖然 Network Manager 會自動修復大部分的安全性弱點，部分修復仍需要您啓動易受入侵電腦上的 SecurityCenter，並遵循所提供的建議。

在遠端電腦上安裝 McAfee 安全性軟體

若您網路上一或多部電腦並未執行 McAfee 2007 安全性軟體，則無法從遠端監視其安全性狀態。若您要從遠端監視這些電腦，您必須到每部電腦並安裝 McAfee 2007 安全性軟體。

若要在遠端電腦上安裝 McAfee 安全性軟體：

1. 於遠端電腦上的瀏覽器中，前往 http://download.mcafee.com/us/。
2. 依照螢幕上的指示在電腦上安裝 McAfee 2007 安全性軟體。

第 13 章

McAfee VirusScan

VirusScan 提供完善、可靠及最新的病毒與間諜軟體防護。VirusScan 使用獲獎的 McAfee 掃描技術，保護您不受病毒、蠕蟲、特洛伊木馬、可疑的指令碼、Rootkit、緩衝區溢位、網路混合式攻擊、間諜軟體、可能無用的程式，以及其他威脅的攻擊或影響。

在本章中

功能

此版本的 VirusScan 提供下列功能。

病毒防護

在您或電腦存取掃描檔時，即時進行掃描。

掃描

在硬碟、磁片以及個別檔案與資料夾中搜尋病毒及其他各種威脅。您也可以在某個項目上按一下滑鼠右鍵，掃描該項目。

間諜軟體與廣告軟體偵測

VirusScan 會識別及移除可能危及您的隱私權、降低您電腦效能的間諜軟體、廣告軟體及其他程式。

自動更新

自動更新能保護您的電腦，遠離最新發現的威脅及不明的威脅。

快速背景掃描

不引人注目的快速掃描能在不中斷您工作的情形下，識別並摧毀病毒、特洛伊病毒、蠕蟲、間諜軟體、廣告軟體、撥號軟體及其他威脅。

即時安全性警告

安全性警告會通知您緊急的病毒爆發和安全性威脅，並提供移除、消除或深入瞭解該威脅的回應選項。

在多個進入點進行偵測和清除

VirusScan 會在電腦的下列主要進入點監視並清除病毒：電子郵件、即時訊息附件及網際網路下載內容。

監視電子郵件是否發生疑似蠕蟲的活動

WormStopper™ 會封鎖特洛伊木馬利用電子郵件寄送蠕蟲至其他電腦，並在不明電子郵件程式傳送電子郵件至其他電腦之前提示您。

監視指令碼是否發生疑似蠕蟲的活動

ScriptStopper™ 會封鎖已知、有害的指令碼不在您的電腦上執行。

McAfee X-ray for Windows

McAfee X-ray 會偵測並刪除隱藏在 Windows 裡的 Rootkit 和其他程式。

緩衝區溢位保護

緩衝區溢位保護會防止緩衝區溢位。當可疑的程式或程序嘗試將超過緩衝區限制數量的資料儲存在您電腦上的緩衝區 (暫時資料儲存區)，因而損毀或覆寫相鄰緩衝區中的有效資料時，即會發生緩衝區溢位。

McAfee SystemGuard

SystemGuard 會檢查電腦的特定行爲來預先察覺病毒、間諜軟體或駭客活動。

第 14 章

管理病毒保護

您可以管理即時病毒、間諜軟體、SystemGuard 及指令碼保護。例如，您可以停用掃描功能，或是指定要掃描的項目。

唯有具系統管理員權限的使用者，才能修改進階選項。

在本章中

使用病毒保護

病毒保護 (即時掃描) 功能啟動時，會持續監視您的電腦是否有病毒活動。即時掃描功能會在您或您的電腦存取檔案時掃描檔案。當病毒保護功能偵測到受感染的檔案時，會嘗試清除或移除感染的病毒。如果無法清除或移除檔案，會出現警示來提示您採取進一步的動作。

相關主題

- 瞭解安全性警示 (第 99 頁)

停用病毒保護

如果您停用病毒保護，電腦將不會持續監視病毒活動。如果必須停止病毒保護，請確定您沒有與網際網路連線。

> **注意：**停用病毒保護也會停用即時間諜軟體、電子郵件及即時訊息保護。

若要停用病毒保護：

1 按一下 [進階功能表]上的 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 按一下 [病毒保護] 底下的 [關閉]。

4 在確認對話方塊中執行下列步驟：
   - 若要在一段指定時間後重新啟動病毒保護，請選取 [在此時間之後重新啟用即時掃描] 核取方塊，然後從功能表中選取時間。
   - 若要停止病毒保護在指定時間後重新啟動，請清除 [在此時間之後重新啟用即時掃描] 核取方塊。

5 按一下 [確定]。

如果設定在 Windows 啟動時啟動即時保護，則在您重新啟動電腦後，電腦就會受到保護。

相關主題

- 設定即時保護 (第 72 頁)

啓用病毒保護

病毒保護會持續監視您的電腦是否有病毒活動。

若要啓用病毒保護：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 在 [病毒保護] 之下，按一下 [開啓]。

設定即時保護

您可以修改即時病毒保護。例如，可以只掃描程式檔案和文件，或者在 Windows 啟動時停用即時掃描 (不建議使用)。

設定即時保護

您可以修改即時病毒保護。例如，可以只掃描程式檔案和文件，或者在 Windows 啟動時停用即時掃描 (不建議使用)。

若要設定即時保護：

1 按一下 [進階功能表]上的 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 按一下 [病毒保護] 底下的 [進階]。

4 選取或清除下列核取方塊：

- **使用啓發式技術來掃描不明病毒**：檔案會和已知病毒的簽章比對，以偵測未識別之病毒的跡象。此選項提供了最徹底的掃描，但是速度通常會比普通掃描慢。
- **關機時掃描軟碟機**：您關閉電腦時，會掃描軟碟機。
- **掃描間諜軟體及潛在無用程式**：會偵測及移除可能在未經您許可之下，收集並傳輸資料的間諜軟體、廣告軟體及其他程式。
- **掃描並移除追蹤 Cookie**：會偵測及移除可能在未經您許可之下收集並傳輸資料的 Cookie。Cookie 會在使用者瀏覽網頁時識別使用者。
- **掃描網路磁碟機**：會掃描連接到您網路的磁碟機。
- **啓用緩衝區溢位保護**：如果偵測到緩衝區溢位活動，會封鎖活動並向您警示。
- **當 Windows 啓動時，啓動即時掃描 (建議使用)**：即使您在階段作業時關閉即時保護，仍會在您每次啓動電腦時啓用即時保護。

5 按一下下列其中一個按鈕：

- **所有檔案 (建議使用)**：會掃描您的電腦使用的每一種檔案類型。使用此選項進行最徹底的掃描。
- **僅程式檔案及文件**：只掃描程式檔案及文件。

6 按一下 [確定]。

使用間諜軟體保護

間諜軟體保護會移除間諜軟體、廣告軟體，以及其他未經您允許即逕自收集和傳輸資料的潛在無用程式。

停用間諜軟體保護

若您停用間諜軟體保護，就不會偵測未經您允許即逕自收集和傳輸資料的潛在無用程式。

若要停用間諜軟體保護：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 在 [間諜軟體保護] 之下，按一下 [關閉]。

啓用間諜軟體保護

間諜軟體保護會移除間諜軟體、廣告軟體，以及其他未經您允許即逕自收集和傳輸資料的潛在無用程式。

若要啓用間諜軟體保護：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 在 [間諜軟體保護] 之下，按一下 [開啓]。

使用 SystemGuard

SystemGuard 會偵測電腦上可能未經授權的變更，並在發生變更時警示您。稍後您可以檢視並決定是否允許這些變更。

SystemGuard 的分類如下。

程式

程式 SystemGuard 會偵測對啓動檔、延伸模組及設定檔的變更。

Windows

Windows SystemGuard 會偵測對 Internet Explorer 設定值的變更，包括瀏覽器屬性，以及安全性設定。

瀏覽器

瀏覽器 SystemGuard 會偵測對 Windows® 服務、憑證及設定檔的變更。

停用 SystemGuard

若您停用 SystemGuard，就不會偵測電腦上可能未經授權的變更。

若要停用所有 SystemGuard：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電腦與檔案]。
3 在 [SystemGuard 保護] 之下，按一下 [關閉]。

啓用 SystemGuard

SystemGuard 會偵測電腦上可能未經授權的變更，並在發生變更時警示您。

若要啓用 SystemGuard：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電腦與檔案]。
3 在 [SystemGuard 保護] 之下，按一下 [開啓]。

設定 SystemGuard

您可以修改 SystemGuard。您可以針對所偵測到的每一項變更，決定是否要警示您並記錄事件、僅記錄事件，或是停用 SystemGuard。

設定 SystemGuard

您可以修改 SystemGuard。您可以針對所偵測到的每一項變更，決定是否要警示您並記錄事件、僅記錄事件，或是停用 SystemGuard。

若要設定 SystemGuard：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 在 [SystemGuard 保護] 之下，按一下 [進階]。

4 在 SystemGuard 清單中，按一下類別，檢視與 SystemGuard 及其狀態相關的清單。

5 按一下 SystemGuard 的名稱。

6 在 [詳細資料] 之下，檢視 SystemGuard 的相關資訊。

7 在 [我要] 之下，執行下列其中一項動作：

- 如果您想要在發生變更時收到警示並記錄事件，請按一下 [顯示警示]。
- 如果您不想在偵測到變更時採取行動，請按一下 [僅記錄變更]。這樣就只會記錄變更。
- 按一下 [停用這個 SystemGuard] 以關閉 SystemGuard。發生變更時，不會警示您，也不會記錄事件。

8 按一下 [確定]。

瞭解 SystemGuard

SystemGuard 會偵測電腦上可能未經授權的變更，並在發生變更時警示您。稍後您可以檢視並決定是否允許這些變更。

SystemGuard 的分類如下。

程式

程式 SystemGuard 會偵測對啟動檔、延伸模組及設定檔的變更。

Windows

Windows SystemGuard 會偵測對 Internet Explorer 設定值的變更，包括瀏覽器屬性，以及安全性設定。

瀏覽器

瀏覽器 SystemGuard 會偵測對 Windows® 服務、憑證及設定檔的變更。

關於程式 SystemGuard

程式 SystemGuard 會偵測下列項目。

ActiveX 安裝

偵測透過 Internet Explorer 下載的 ActiveX 程式。ActiveX 程式會從網站下載，並儲存在電腦的 C:\Windows\Downloaded Program Files 或 C:\Windows\Temp\Temporary Internet Files 中。也會在系統登錄中以其 CLSID (大括弧內的一長串數字) 來參照它們。

Internet Explorer 會使用許多合法的 ActiveX 程式。如果您不確定 ActiveX 程式的功能，可加以刪除，不會損及電腦。如果您之後還需要此程式，下次您回到需要它的網站時，Internet Explorer 會自動將其下載。

啟動項目

監視對啟動登錄機碼及資料夾所做的變更。Windows 登錄中的啟動登錄機碼，以及 [開始] 功能表中的啟動資料夾，會將程式的路徑儲存在您的電腦上。Windows 啟動時，會載入這些位置中所列的程式。間諜軟體或其他潛在無用程式通常會試著在 Windows 啟動時載入。

Windows Shell 執行攔截

監視對 explorer.exe 中載入的程式清單所做的變更。Shell 執行攔截是載入至 explorer.exe Windows Shell 的程式。Shell 執行攔截程式會接收在電腦上執行的所有執行命令。在實際啓動另一個程式之前，explorer.exe Shell 中載入的任何程式都可先執行其他工作。間諜軟體或其他潛在無用的程式可使用 Shell 執行攔截來防止執行安全性程式。

Shell 服務物件延遲載入

監視對列在 [Shell 服務物件延遲載入] 中之檔案的變更。電腦啓動時，explorer.exe 便會載入這些檔案。因爲 explore.exe 是電腦的 Shell，所以它一定會啓動並載入此機碼之下的檔案。發生任何人爲介入之前，在啓動程序前面階段便已載入這些檔案。

關於 Windows SystemGuard

Windows SystemGuard 會偵測下列項目。

內容功能表處理程式

防止未授權變更 Windows 內容功能表。這些功能表可以讓您在檔案上按一下滑鼠右鍵，執行與該檔案相關的特定動作。

AppInit DLLs

防止未授權變更或增加 Windows AppInit.DLLs。AppInit_DLLs 登錄值包含 user32.dll 載入時所載入的檔案清單。AppInit_DLLs 值當中的檔案會在 Windows 啓動常式的一開始就載入，因此在任何人爲介入之前，有害的 .DLL 可能會先自行隱藏。

Windows 主機檔案

監視對電腦主機檔案的變更。主機檔案是用來將特定的網域名稱重新導向至特定的 IP 位址。例如，當您造訪 www.example.com 時，瀏覽器會檢查主機檔案，尋找 example.com 的項目，然後指向該網域的 IP 位址。有些間諜軟體程式會試圖變更主機檔案，將瀏覽器重新導向另一個網站，或防止軟體適當地更新。

Winlogon Shell

監視 Winlogon Shell。這個 Shell 是在使用者登入 Windows 時載入。Shell 是用來管理 Windows 的主要使用者介面 (UI)，通常是 Windows 檔案總管 (explore.exe)。但是，可以輕易變更 Windows Shell，使其指向另一個程式。如果發生此情形，則每次使用者登入時，啓動的程式就不會是 Windows Shell。

Winlogon User Init

監視對 Windows 登入使用者設定的變更。機碼 HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit 指定在使用者登入 Windows 之後所啓動的程式。預設程式會還原您的設定檔、字型、色彩，以及您的使用者名稱的其他設定。間諜軟體和其他潛在無用的程式可能將自己加入此機碼以嘗試啓動。

Windows 通訊協定

監視對您的網路通訊協定的變更。有些間諜軟體或其他潛在無用程式會控制電腦傳送及接收資訊的特定方式。這是透過 Windows 通訊協定篩選器和處理常式來完成。

Winsock 階層服務提供者

監視階層服務提供者 (LSP)，這些提供者可能在網路上攔截您的資料，並且變更或將資料重新導向。正常的 LSP 包括未成年保護軟體、防火牆，以及其他安全性程式。間諜軟體可以使用 LSP 監視您的網際網路活動，修改您的資料。若要避免重新安裝作業系統，請使用 McAfee 程式自動移除間諜軟體和有害的 LSP。

Windows Shell Open Commands

防止對 Windows Shell (explorer.exe) Open Commands 進行變更。Shell Open Commands 允許特定程式在每次執行特定類型的檔案時執行。例如，蠕蟲可能嘗試在每次執行 .exe 應用程式時執行。

共用工作排程器

監視 SharedTaskScheduler 登錄機碼，此機碼包含在 Windows 啓動時執行的程式清單。有些間諜軟體或其他潛在無用程式會修改此機碼，並在未經您許可的情形下將自己新增至清單中。

Windows Messenger Service

監視 Windows Messenger Service，該服務是未記載的 Windows Messenger 功能，可以讓使用者傳送快顯式訊息。有些間諜軟體或其他潛在無用程式會嘗試啓用該服務，並傳送來路不明的廣告。也可以使用已知弱點，利用此服務從遠端執行程式碼。

Windows Win.ini 檔案

win.ini 檔案是文字檔，它提供 Windows 啓動時執行之程式的清單。此檔案含有載入這些程式的語法，以支援舊版的 Windows。大部分程式都不使用 sin.ini 檔案載入程式：不過，有些間諜軟體或其他潛在無用程式的設計會利用此語法，並在 Windows 啓動時自行載入。

關於瀏覽器 SystemGuard

瀏覽器 SystemGuard 會偵測下列項目。

瀏覽器協助程式物件

監視瀏覽器協助程式物件 (BHO) 的新增項目。BHO 是作爲 Internet Explorer 外掛程式的程式。間諜軟體和瀏覽器駭客通常使用 BHO 來顯示廣告，或追蹤您的瀏覽習慣。許多合法程式也使用 BHO，例如一般搜尋工具列。

Internet Explorer 列

監視對 Internet Explorer 列程式清單所做的變更。瀏覽器列是一個窗格，類似您在 Internet Explorer (IE) 或 Windows 檔案總管中看到的 [搜尋]、[我的最愛] 或 [記錄] 窗格。

Internet Explorer 外掛程式

防止間諜軟體安裝 Internet Explorer 外掛程式。Internet Explorer 外掛程式是在 Internet Explorer 啓動時載入的附加元件。間諜軟體通常使用 Internet Explorer 外掛程式來顯示廣告，或追蹤您的瀏覽習慣。合法的外掛程式會爲 Internet Explorer 增加功能。

Internet Explorer ShellBrowser

監視對 Internet Explorer ShellBrowser 例項所做的變更。Internet Explorer ShellBrowser 包含 Internet Explorer 之例項的資訊和設定。如果變更這些設定或新增了 ShellBrowser，這個 ShellBrowser 可完全控制 Internet Explorer，加入工具列、功能表及按鈕等功能。

Internet Explorer WebBrowser

監視對 Internet Explorer WebBrowser 例項所做的變更。Internet Explorer WebBrowser 包含關於 Internet Explorer 例項的資訊及設定。如果變更這些設定或新增了 WebBrowser，這個 WebBrowser 可完全控制 Internet Explorer，加入工具列、功能表及按鈕等功能。

Internet Explorer URL 搜尋攔截

監視對 Internet Explorer URL 搜尋攔截所做的變更。當您在瀏覽器的位置欄位中輸入位址，但是位址中沒有 http:// 或 ftp:// 等通訊協定時，會使用 URL 搜尋攔截。當您輸入這樣的位址時，瀏覽器可能使用 UrlSearchHook 來搜尋網際網路，以找出您輸入的位置。

Internet Explorer URL

監視對 Internet Explorer 預設 URL 所做的變更。這會防止間諜軟體或其他潛在無用之程式，未經您的許可就變更瀏覽器的設定。

Internet Explorer 限制

監視 Internet Explorer 限制，這些限制可以讓電腦管理員防止使用者變更 Internet Explorer 裡的首頁或其他選項。唯有您的系統管理員刻意設定這些選項時，選項才會出現。

Internet Explorer 安全區域

監視 Internet Explorer 安全區域。Internet Explorer 有四個預先定義的安全區域：網際網路、近端內部網路、信任的網站和限制的網站。每一個安全區域有它自己的安全設定，這些設定是預先定義或自訂的。安全區域是某些間諜軟體或其他潛在無用程式的目標，因為降低安全層級可讓這些程式略過安全性警示而不被發現。

Internet Explorer 信任的網站

監視 Internet Explorer 信任的網站。信任的網站清單是您信任之網站的目錄。有些間諜軟體或其他潛在無用程式以此清單為目標，因為它提供方法，未經過您的許可就信任可疑網站。

Internet Explorer 政策

監視 Internet Explorer 政策。這些設定通常是由系統管理員變更，但是間諜軟體可能會入侵這些設定。變更可能會阻止您設定其他首頁，或者可能隱藏 [工具] 功能表 [網際網路選項] 對話方塊中的索引標籤，讓您看不見。

使用指令碼掃描

指令碼可建立、複製或刪除檔案，亦可開啟您的 Windows 登錄。

指令碼掃描會自動防止已知有害的指令碼在您的電腦上執行。

停用指令碼掃描

若您停用指令碼掃描，就不會偵測可疑的指令碼執行狀況。

若要停用指令碼掃描：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電腦與檔案]。
3 在 [指令碼掃描保護] 之下，按一下 [關閉]。

啟用指令碼掃描

如果有指令碼執行，並導致建立、複製或刪除檔案，或者開啟您的 Windows 登錄，指令碼掃描就會警示您。

若要啟用指令碼掃描：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電腦與檔案]。
3 在 [指令碼掃描保護] 之下，按一下 [開啟]。

使用電子郵件保護

電子郵件保護會偵測並防止入埠 (POP3) 及出埠 (SMTP) 電子郵件訊息及附件中的威脅，包括病毒、特洛依病毒、蠕蟲、間諜軟體、廣告軟體和其他威脅。

停用電子郵件保護

若您停用電子郵件保護，就不會偵測入埠 (POP3) 及出埠 (SMTP) 電子郵件訊息及附件中的潛在威脅。

若要停用電子郵件保護：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。
3 在 [電子郵件保護] 之下，按一下 [關閉]。

啓用電子郵件保護

電子郵件保護會偵測入埠 (POP3) 及出埠 (SMTP) 電子郵件訊息與附件中的威脅。

若要啓用電子郵件保護：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。
3 在 [電子郵件保護] 之下，按一下 [開啓]。

設定電子郵件保護

電子郵件訊息保護選項可讓您掃描入埠電子郵件訊息、出埠電子郵件訊息及蠕蟲。蠕蟲會複製並消耗系統資源，進而降低效能或中止工作。蠕蟲會透過電子郵件訊息來傳送自己的副本。例如，它會嘗試將電子郵件訊息轉寄給您通訊錄中的人員。

設定電子郵件保護

電子郵件訊息保護選項可讓您掃描入埠電子郵件訊息、出埠電子郵件訊息及蠕蟲。

若要設定電子郵件保護：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 在 [電子郵件保護] 之下，按一下 [進階]。

4 選取或清除下列核取方塊：

- **掃描入埠電子郵件訊息**：掃描入埠 (POP3) 訊息是否有潛在的威脅。
- **掃描出埠電子郵件訊息**：掃描出埠 (SMTP) 訊息是否有潛在的威脅。
- **啟用 WormStopper**：WormStopper 可封鎖電子郵件訊息中的蠕蟲。

5 按一下 [確定]。

使用即時訊息保護

即時訊息保護會偵測入埠即時訊息附件中的威脅。

停用即時訊息保護

若您停用即時訊息保護，就不會偵測入埠即時訊息附件中的威脅。

若要停用即時訊息保護：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 在 [即時訊息保護] 之下，按一下 [關閉]。

啓用即時訊息保護

即時訊息保護會偵測入埠即時訊息附件中的威脅。

若要啓用即時訊息保護：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 在 [即時訊息保護] 之下，按一下 [開啓]。

第 15 章

手動掃描電腦

您可以在硬碟、磁片以及個別檔案和資料夾中，搜尋病毒及其他威脅。VirusScan 發現可疑的檔案時，除非是潛在的無用程式，否則會嘗試清除檔案中的病毒。如果 VirusScan 無法清除檔案中的病毒，您可以將檔案隔離或刪除。

在本章中

手動掃描

您隨時都可以手動掃描。例如，若您才剛安裝 VirusScan，則可以執行掃描以確保電腦中沒有任何病毒或其他威脅。或者，若您已停用即時掃描，則可以執行掃描以確保電腦仍是安全的。

使用手動掃描設定來掃描

這類型的掃描會使用您指定的手動掃描設定。VirusScan 會掃描內部的壓縮檔 (.zip、.cab 等等)，但是一個壓縮檔只算成一個檔案。同樣的，如果您刪除了自上次掃描以後的暫存網際網路檔案，所掃描的檔案的數目可能會不同。

若要使用手動掃描設定來掃描：

1 在 [基本功能表] 上，按一下 [掃描]。完成掃描時，摘要會顯示所掃描及偵測的項目數、已清除病毒的項目數，以及最後一次掃描的時間。

2 按一下 [完成]。

相關主題

- 設定手動掃描 (第 90 頁)

不使用您的手動掃描設定掃描

這類掃描不會使用您指定的手動掃描設定。VirusScan 會掃描內部壓縮檔 (.zip、.cab 等)，但是一個壓縮檔只算成一個檔案。同樣的，如果您刪除了自上次掃描以後的暫存網際網路檔案，所掃描的檔案的數目可能會不同。

若要不使用您的手動掃描設定掃描：

1 按一下 [進階功能表]上的 [首頁]。

2 按一下 [首頁] 窗格上的 [掃描]。

3 在 [要掃描的位置] 底下，選取您要掃描之檔案、資料夾和磁碟機旁的核取方塊。

4 在 [選項] 底下，選取您要掃描之檔案類型旁的核取方塊。

5 按一下 [立即掃描]。掃描完成後，有一個摘要會顯示掃描和偵測到的項目數、清除的項目數，以及上次掃描的時間。

6 按一下 [完成]。

注意：這些選項不會儲存。

在 Windows 檔案總管中掃描

您可以在 Windows 檔案總管中掃描所選取之檔案、資料夾或磁碟機中的病毒及其他威脅。

若要在 Windows 檔案總管中掃描檔案：

1. 開啓 Windows 檔案總管。
2. 在要掃描的檔案、資料夾或磁碟機上按一下滑鼠右鍵，然後按一下 [掃描]。選取所有預設掃描選項可提供徹底的掃描。

設定手動掃描

在執行手動或排程掃描時，您可以指定要掃描的檔案類型、位置，以及要執行掃描的時間。

設定要掃描的檔案類型

您可以設定要掃描的檔案類型。

若要設定掃描的檔案類型：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 在 [病毒保護] 之下，按一下 [進階]。

4 在 [病毒保護] 窗格上，按一下 [手動掃描]。

5 選取或清除下列核取方塊：

- **使用啓發式技術來掃描不明病毒**：核對檔案是否具有已知病毒的簽章，以偵測不明病毒的簽章。此選項提供了最徹底的掃描，但是速度通常會比普通掃描慢。
- **掃描 .zip 及其他封存檔**：偵測及移除 .zip 和其他封存檔中的病毒。有時候，病毒作者會將病毒放在 .zip 檔案中，然後將該 .zip 檔案插入另一個 .zip 檔案中，以逃過防毒掃描程式的掃描。
- **掃描間諜軟體及潛在無用程式**：偵測並移除間諜軟體、廣告軟體，以及可能未經您允許即收集並傳輸資料的其他程式。
- **掃描並移除追蹤 Cookie**：偵測並移除可能未經您允許即收集並傳輸資料的 Cookie。Cookie 可在使用者瀏覽網頁時，識別使用者。
- **掃描 Rootkit 及其他隱形程式**：偵測並移除隱藏起來不被 Windows 發現的任何 Rootkit 及其他程式。

6 按一下底下其中一個按鈕：

- **所有檔案 (建議使用)**：將會掃描您電腦所使用的每一種檔案類型。請使用此選項以進行最徹底的掃描。
- **僅程式檔及文件**：僅掃描程式檔及文件。

7 按一下 [確定]。

設定要掃描的位置

您可以針對手動或排程掃描，設定所要掃描的位置。

若要設定掃描的位置：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電腦與檔案]。
3 在 [病毒保護] 之下，按一下 [進階]。
4 在 [病毒保護] 窗格上，按一下 [手動掃描]。
5 在 [要掃描的預設位置] 之下，選取您要掃描的檔案、資料夾及磁碟機。

   若要獲得最徹底的掃描，請確定已選取 [重要檔案]。
6 按一下 [確定]。

排程掃描

您可以排定掃描的時程，依所指定的時間間隔來徹底檢查電腦中的病毒及其他威脅。

若要排定掃描：

1 在 [進階功能表]上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電腦與檔案]。
3 在 [病毒保護] 之下，按一下 [進階]。
4 在 [病毒保護] 窗格上，按一下 [排程掃描]。
5 確定已選取 [啓用排程掃描]。
6 選擇您要在星期幾執行掃描，選取那一天旁的核取方塊。
7 按一下開始時間清單中的值，以指定開始時間。
8 按一下 [確定]。

秘訣： 若要使用預設排程，請按一下 [重設]。

第 16 章

管理 VirusScan

您可以移除信任清單中的項目、管理隔離的程式、Cookie 和檔案、檢視事件和記錄檔，以及向 McAfee 報告可疑的活動。

在本章中

管理信任的清單

當您信任 SystemGuard、程式、緩衝區溢位或電子郵件程式時，將該項目加入信任的清單後，就不會再偵測這些項目。

如果您誤信了某個程式，或是想要偵測該程式，您必須將它從這個清單中移除。

管理信任的清單

當您信任 SystemGuard、程式、緩衝區溢位或電子郵件程式時，將該項目加入信任的清單後，就不會再偵測這些項目。

如果您誤信了某個程式，或是想要偵測該程式，您必須將它從這個清單中移除。

若要從信任的清單中移除項目：

1 在 [進階功能表]上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電腦與檔案]。

3 在 [病毒保護] 之下，按一下 [進階]。

4 在 [病毒保護] 窗格上，按一下 [信任清單]。

5 在清單中選取信任的 SystemGuard、程式、緩衝區溢位或電子郵件程式，檢視其項目及項目的信任狀態。

6 在 [詳細資料] 之下，檢視項目的相關資訊。

7 在 [我要] 之下，點選一個動作。

8 按一下 [確定]。

管理隔離的程式、Cookie 及檔案

您可以將隔離的程式、Cookie 及檔案還原、刪除，或是傳送至 McAfee 進行分析。

還原隔離的程式、Cookie 及檔案

若有必要，您可以還原隔離的程式、Cookie 及檔案。

若要還原隔離的程式、Cookie 及檔案：

1 在 [進階功能表]上，按一下 [還原]。
2 在 [還原] 窗格上，視情況按一下 [程式及 Cookie] 或 [檔案]。
3 選取您要還原的隔離程式、Cookie 及檔案。
4 如需所隔離之病毒的詳細資訊，請在 [詳細資料] 之下，按一下該病毒的偵測名稱。隨即出現 [病毒資訊庫] 及病毒說明。
5 在 [我要] 之下，按一下[還原]。

移除隔離的程式、Cookie 及檔案

您可以移除隔離的程式、Cookie 及檔案。

若要移除隔離的程式、Cookie 及檔案：

1 在 [進階功能表]上，按一下 [還原]。
2 在 [還原] 窗格上，視情況按一下 [程式及 Cookie] 或 [檔案]。
3 選取您要還原的隔離程式、Cookie 及檔案。
4 如需所隔離之病毒的詳細資訊，請在 [詳細資料] 之下，按一下該病毒的偵測名稱。隨即出現 [病毒資訊庫] 及病毒說明。
5 在 [我要] 之下，按一下[移除]。

傳送隔離的程式、Cookie 及檔案至 McAfee

您可以將隔離的程式、Cookie 及檔案傳送至 McAfee 進行分析。

注意：如果您所傳送的隔離檔超過大小上限，檔案會被退回。在大部分情況下，並不會發生這種情況。

若要傳送隔離的程式或檔案至 McAfee：

1 在 [進階功能表]上，按一下 [還原]。
2 在 [還原] 窗格上，視情況按一下 [程式及 Cookie] 或 [檔案]。
3 選取您要傳送至 McAfee 的隔離程式、Cookie 及檔案。
4 如需所隔離之病毒的詳細資訊，請在 [詳細資料] 之下，按一下該病毒的偵測名稱。隨即出現 [病毒資訊庫] 及病毒說明。
5 在 [我要] 之下，按一下[傳送至 McAfee]。

檢視最近的事件及記錄檔

最近的事件及記錄檔會顯示所安裝之所有 McAfee 產品的事件。

您可以在 [最近的事件] 之下，看到您電腦上最近發生的前 30 項重大事件。您可以還原封鎖的程式、重新啓用即時掃描及信任緩衝區溢位。

您也可以檢視記錄檔，其中記錄了最近 30 天所發生的每個事件。

檢視事件

您可以在 [最近的事件] 之下，看到您電腦上最近發生的前 30 項重大事件。您可以還原封鎖的程式、重新啓用即時掃描及信任緩衝區溢位。

若要檢視事件：

1 在 [進階功能表]上，按一下 [報告與記錄]。

2 在 [報告與記錄] 窗格上，按一下 [最近的事件]。

3 選擇您要檢視的事件。

4 在 [詳細資料] 之下，檢視該事件的相關資訊。

5 在 [我要] 之下，點選一個動作。

檢視記錄檔

記錄檔記錄了最近 30 天所發生的每個事件。

若要檢視記錄檔：

1 在 [進階功能表]上，按一下 [報告與記錄]。

2 在 [報告與記錄] 窗格上，按一下 [最近的事件]。

3 在 [最近的事件] 窗格上，按一下 [檢視記錄檔]。

4 選取您要檢視的記錄檔類型，然後選取一個記錄檔。

5 在 [詳細資料] 之下，檢視記錄檔的相關資訊。

自動報告匿名資訊

您可以將病毒、潛在的無用程式及駭客追蹤資訊匿名傳送給 McAfee。這個選項只有在安裝期間可供使用。

不會收集任何個人的識別資訊。

報告至 McAfee

您可以將病毒、潛在的無用程式及駭客追蹤資訊傳送給 McAfee。這個選項只有在安裝期間可供使用。

若要自動報告匿名資訊：

1 在 VirusScan 安裝期間，接受預設的 [傳送匿名資訊]。

2 按一下 [下一步]。

瞭解安全性警示

如果即時掃描偵測到威脅，即會顯示警示。對於大部份的病毒、特洛伊病毒、指令碼及蠕蟲，即時掃描都會自動嘗試清除檔案中的病毒，並警示您。針對潛在的無用程式及 SystemGuard，即時掃描會偵測檔案或變更，並警示您。對於緩衝區溢位、追蹤 Cookie 及指令碼活動，即時掃描會自動封鎖該活動，並警示您。

這些警示可分成三種基本類型。

- 紅色警示
- 黃色警示
- 綠色警示

您可以選擇如何管理所偵測的檔案、所偵測的電子郵件、可疑的指令碼、潛在的蠕蟲、潛在的無用程式、SystemGuard 或緩衝區溢位。

管理警示

McAfee 使用一系列警示來協助您管理安全性。這些警示可分成三種基本類型。

- 紅色警示
- 黃色警示
- 綠色警示

紅色警示

紅色警示需要您的回應。在某些情況下，McAfee 無法判斷如何自動回應特定的活動。在這種情況下，紅色警示會以問題型式來描述活動，並提供一或多個選項供您選取。

黃色警示

黃色警示是不嚴重的通知，通常會需要您的回應。黃色警示會以問題型式來描述活動，並提供一或多個選項供您選取。

綠色警示

在大多數的情況下，綠色警示會提供事件的基本相關資訊，且不需要回應。

設定警示選項

如果您選擇不再顯示警示，但稍後又改變心意，您可以再回頭設定爲要顯示警示。如需有關設定警示選項的詳細資訊，請參閱 SecurityCenter 說明文件。

第 17 章

其他說明

本章說明常見問題及疑難排解案例。

在本章中

常見問題集

本節提供最常見之問題的解答。

偵測到威脅，該如何處理？

McAfee 使用警示幫助您管理安全性。這些警示可以分成三種基本類型。

- 紅色警示
- 黃色警示
- 綠色警示

您可以選擇如何管理偵測到的檔案、偵測到的電子郵件、可疑的指令碼、潛在的蠕蟲、潛在的無用程式、SystemGuard 或緩衝區溢位。

如需有關管理特定威脅的詳細資訊，請參閱 Virus Information Library (病毒資訊庫)，網址為：http://tw.mcafee.com/virusInfo/。

相關主題

- 瞭解安全性警告 (第 99 頁)

我可以使用 VirusScan 來搭配 Netscape、Firefox 或 Opera 瀏覽器嗎？

您可以使用 Netscape、Firefox 及 Opera 來作為您的預設網際網路瀏覽器，但是您的電腦上必須裝有 Microsoft® Internet Explorer 6.0 或更新的版本。

我需要連接至網際網路才能執行掃描嗎？

您不需要連接至網際網路即可執行掃描，但是您一星期至少要連接一次以接收 McAfee 更新。

VirusScan 會掃描電子郵件附件嗎？

若您已啟用即時掃描及電子郵件保護，當電子郵件訊息到達時，即會掃描任何附件。

VirusScan 會掃描壓縮檔嗎？

VirusScan 會掃描 .zip 檔及其他封存檔。

爲什麼會出現出埠電子郵件掃描錯誤？

在掃描出埠電子郵件訊息時，可能會發生以下類型的錯誤：

- 通訊協定錯誤。電子郵件伺服器拒絕了電子郵件訊息。
  如果發生通訊協定錯誤或系統錯誤，仍會處理該工作階段的其餘電子郵件訊息，並將其傳送至伺服器。
- 連線錯誤。連接到電子郵件伺服器的連線已中斷。
  如果發生連線錯誤，請確定電腦有連接至網際網路，然後重新嘗試從電子郵件程式中的 [寄件匣] 項目清單傳送該訊息。
- 系統錯誤。發生檔案處理錯誤或其他系統錯誤。
- 加密的 SMTP 連線錯誤。偵測到來自您電子郵件程式的加密 SMTP 連線。
  如果發生加密的 SMTP 連線錯誤，請將電子郵件程式中加密 SMTP 連線關閉，以確保會對電子郵件訊息進行掃描。

如果在傳送電子郵件訊息時發生逾時，請停用出埠電子郵件掃描，或關閉電子郵件程式中的加密 SMTP 連線。

相關主題

- 設定電子郵件保護 (第 84 頁)

疑難排解

本節針對您可能遇到的一般問題提供協助。

無法清除或刪除病毒

針對某些病毒，您必須手動清理您的電腦。嘗試重新啓動電腦，然後再掃描一次。

如果您的電腦無法清除或刪除病毒，請參閱 Virus Information Library (病毒資訊庫)，網址爲：http://tw.mcafee.com/virusInfo/。

如需其他協助，請洽詢 McAfee 網站上的 McAfee 客戶支援。

注意：無法從 CD-ROM、DVD 及具寫入保護的磁碟片中清除病毒。

重新啓動之後，仍無法移除項目

在某些情況下，掃描及移除項目之後，需要重新啓動電腦。

如果重新啓動電腦之後，仍未移除該項目，請將檔案提交至 McAfee。

注意：無法從 CD-ROM、DVD 及具寫入保護的磁碟片中清除病毒。

相關主題

- 管理隔離的程式、Cookie 及檔案 (第 95 頁)

元件遺失或損毀

有些狀況會導致 VirusScan 安裝錯誤：

- 您的電腦沒有足夠的磁碟空間或記憶體。請確認電腦符合執行這個軟體的系統需求。
- 您網際網路瀏覽器的設定不正確。
- 您的網際網路連線有誤。請檢查連線；或是稍後再嘗試連線。
- 檔案遺失或安裝失敗。

最佳的解決方式，就是解決上述的可能問題，再重新安裝 VirusScan。

第 18 章

McAfee Personal Firewall

Personal Firewall 為您的電腦和個人資料提供進階保護。Personal Firewall 在您的電腦與網際網路之間建立了障礙，秘密監視網際網路流量中是否有可疑的活動。

在本章中

功能

Personal Firewall 可提供完整的入埠和出埠防火牆保護，且會自動信任已知的良好程式，並協助封鎖間諜軟體、特洛伊病毒與按鍵側錄器。Firewall 可讓您抵禦駭客的探測及攻擊、監視網際網路及網路活動、警示您發生有害或可疑的事件、提供網際網路流量的詳細資訊並協助防禦病毒的攻擊。

標準及自訂保護等級

使用 Firewall 的預設保護設定或自訂符合自己安全性需求的 Firewall，來抵抗入侵及可疑的活動。

即時掃描建議

積極的接收建議可幫助您判斷是否要將網際網路存取權授與程式或是否要信任網路流量。

程式的智慧型存取管理

透過警示及事件記錄來管理程式的網際網路存取權，或從 Firewall 的 [程式權限] 窗格設定特定程式的存取權。

遊戲保護

在全螢幕的模式下進行遊戲時，防止入侵嘗試及可疑活動的警示干擾您，並設定 Firewall 在電腦遊戲結束後才顯示警示。

電腦啓動保護

在 Windows 開啓前，Firewall 會保護您的電腦避免入侵嘗試及無用程式和網路流量的攻擊。

系統服務通訊埠控制

系統服務通訊埠可提供後門供電腦使用。Firewall 可讓您建立並管理某些程式需要之開啓及關閉的系統服務通訊埠。

管理電腦連線

信任及禁止可連線到您電腦的遠端連線及 IP 位址。

HackerWatch 資訊整合

HackerWatch 是一種安全性資訊的中樞，可追蹤全球的駭客活動及入侵嘗試，並可提供關於電腦上程式的最新資訊。您可檢視全球的安全性事件及網際網路通訊埠統計資料。

鎖定 Firewall

會立即封鎖電腦和網際網路之間的所有入埠和出埠網際網路流量。

還原 Firewall

立即還原 Firewall 的原始保護設定。如果 Personal Firewall 出現您無法修正的非預期行為，您可將 Firewall 還原為預設設定。

進階特洛伊病毒偵測

將程式連線管理與增強的資料庫相結合，可以偵測和封鎖更多潛在的惡意應用程式 (如特洛伊病毒)，阻止它們存取網際網路和轉送您的個人資料。

事件記錄

可讓您指定是否要啓用或停用記錄，以及指定啓用後所要記錄的事件類型。事件記錄可讓您檢視最近的入埠及出埠事件。您也可以檢視偵測到的入侵事件。

監視網際網路流量

檢閱簡單易讀的圖形化活動圖，其中會顯示全世界惡意攻擊和流量的來源。此外，可尋找起始 IP 位址的擁有者詳細資訊及地理位置資料。同時分析入埠及出埠流量、監視程式頻寬及程式活動。

入侵保護

提供對可能之網際網路威脅的入侵保護，來保護您的隱私。McAfee 使用啓發式功能，透過封鎖顯示攻擊徵兆或入侵企圖特徵的項目，提供第三層保護。

精密的流量分析

同時檢閱入埠及出埠網際網路流量與程式連線，包含正積極接聽開放連線的連線。這可讓您看到容易遭到入侵的程式並對其採取行動。

啓動防火牆

一旦安裝防火牆，就會保護您的電腦避免入侵以及無用的網路流量。此外，您還可以處理警示，並管理已知或不明程式的入埠及出埠網際網路存取。[自動建議] 及 [標準] 安全性層級會自動啓用。

雖然您可以從 [網際網路與網路設定] 窗格停用防火牆，但是停用後將不再繼續保護電腦避免入侵及無用的網路流量，而且也將無法有效管理入埠及出埠的網際網路連線。如果必須停用防火牆保護，請只在需要時暫時停用。您也可以從 [網際網路與網路設定] 窗格啓用防火牆。

這個防火牆會自動停用 Windows® 防火牆，並將自己設爲預設防火牆。

注意：若要設定 Firewall，請開啓 [網際網路與網路設定] 窗格。

啓動防火牆保護

啓用防火牆保護可保護您的電腦避免入侵以及無用的網路流量，並協助您管理入埠及出埠的網際網路連線。

若要啓用防火牆保護：

1 請在 McAfee SecurityCenter 窗格上，執行下列其中一項動作：
   - 按一下 [網際網路與網路]，然後按一下 [設定]。
   - 依序按一下 [進階功能表]、[首頁] 窗格上的 [設定]，然後指向 [網際網路與網路]。
2 在 [網際網路與網路設定] 窗格中的 [防火牆保護] 底下，按一下 [開啓]。

停止防火牆保護

停用防火牆保護會讓您的電腦容易遭到入侵，而且也容易收到無用的網路流量。若沒有啓用防火牆保護，您將無法管理入埠及出埠的網際網路連線。

若要停用防火牆保護：

1 請在 McAfee SecurityCenter 窗格上，執行下列其中一項動作：
   - 按一下 [網際網路與網路]，然後按一下 [設定]。

- 依序按一下 [進階功能表]、[首頁] 窗格上的 [設定]，然後指向 [網際網路與網路]。

2 在 [網際網路與網路設定] 窗格中的 [防火牆保護] 底下，按一下 [關閉]。

使用警示

防火牆使用一系列警示，協助您管理安全性。這些警示可以分成四個基本類型。

- 已封鎖特洛伊病毒警示
- 紅色警示
- 黃色警示
- 綠色警示

警示也可能包含下列用途的資訊：協助使用者決定如何處理警示，或取得在其電腦上執行之程式的相關資訊。

關於警示

防火牆具有四個基本警示類型。有些警示包含的資訊也可協助您瞭解或取得在您電腦上執行之程式的相關資訊。

已封鎖特洛伊病毒警示

特洛伊病毒看似合法的程式，卻會干擾、損壞您的電腦，以及提供未經授權的存取電腦管道。當防火牆在您電腦上偵測到特洛伊病毒時，會出現特洛伊病毒警示並封鎖特洛伊病毒，然後建議您掃描其他威脅。這個警示會出現在每個安全性層級中，但 [開放] 或停用 [自動建議] 時除外。

紅色警示

最常見的警示類型為紅色警示，通常需要您有所回應。因為防火牆在某些情況下無法自動判斷應針對程式活動或網路事件採取的一連串動作，所以警示會先說明有問題的程式活動或網路事件，然後顯示一個或多個您必須回應的選項。如果已啓用 [自動建議]，則程式會新增至 [程式權限] 窗格。

以下是最常遇到的警示說明：

- **程式要求網際網路存取權**：防火牆偵測到程式正在嘗試存取網際網路。
- **程式已修改**：防火牆偵測到已經歷某種變更的程式，這也許是因為線上更新所致。
- **封鎖的程式**：防火牆會封鎖程式，因為它列在 [程式權限] 窗格上。

以下是最常遇到的選項，視您的設定及程式活動或網路事件而定：

- **授予存取權**：允許您電腦上的程式存取網際網路。這個規則會新增至 [程式權限] 頁。
- **授予存取權一次**：允許您電腦上的程式暫時存取網際網路。例如，安裝新程式可能只需要存取一次。
- **封鎖存取**：防止程式存取網際網路。
- **授予限出埠存取權**：只允許網際網路的出埠連線。通常當設定 [嚴密] 及 [秘密] 安全性層級時，便會出現這個警示。
- **信任此網路**：允許來自網路的入埠及出埠流量。網路會新增至 [信任的 IP 位址] 區段。
- **此時不要信任此網路**：封鎖來自網路的入埠及出埠流量。

黃色警示

黃色警示是無關緊要的通知，它會通知您有關防火牆偵測到的網路事件。例如，當防火牆第一次執行時，或當已安裝防火牆的電腦連線至新網路時，[偵測到新網路] 警示便會出現。您可以選擇信任或不信任網路。如果信任網路，防火牆將允許來自網路上任何電腦的流量，並會新增至 [信任的 IP 位址]。

綠色警示

在大多數情況下，綠色警示提供有關事件的基本資訊，而且不需要回應。當設定 [標準]、[嚴密]、[秘密] 及 [鎖定] 安全性層級時，通常會出現綠色警示。綠色警示說明如下：

- **程式已修改**：通知您先前允許存取網際網路的程式已遭到修改。您可以選擇封鎖程式，但是如果您沒有回應，警示會從桌面消失，而程式會繼續具有存取權。
- **被授予網際網路存取權的程式**：通知您已授予程式網際網路存取權。您可以選擇封鎖程式，但是如果您沒有回應，警示會消失，而程式會繼續存取網際網路。

使用者幫助

許多防火牆警示包含其他可協助您管理電腦安全性的資訊，包括：

- **深入瞭解有關此程式的資訊**：啓動 McAfee 的全球安全性網站，取得防火牆在您電腦上偵測到的程式的相關資訊。
- **通知 McAfee 關於此程式的資訊**：將防火牆在您電腦上偵測到的不明檔案的相關資訊傳送至 McAfee。
- **McAfee 建議**：有關處理警示的建議。例如，警示可能會建議您將存取權授予程式。

管理資訊警示

防火牆可讓您在發生某些事件期間顯示或隱藏資訊警示。

玩遊戲時顯示警示

依預設，防火牆會防止資訊警示在全螢幕玩遊戲期間出現。但是，您可以設定防火牆，讓防火牆在您玩遊戲期間偵測到入侵嘗試或可疑的活動時，顯示資訊警示。

若要在玩遊戲期間顯示警示：

1 在 [常見工作] 窗格上，按一下 [進階功能表]。
2 按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [警示]。
4 按一下 [進階]。
5 在 [警示選項] 窗格上，選取 [偵測到遊戲模式時，顯示資訊警示]。

隱藏資訊警示

資訊警示會通知有關不需立即注意的事件。

若要隱藏資訊警示：

1 在 [常見工作] 窗格上，按一下 [進階功能表]。
2 按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [警示]。
4 按一下 [進階]。
5 在 [SecurityCenter 設定] 窗格上，按一下 [資訊警示]。
6 在 [資訊警示] 窗格上，執行下列其中一項動作：
   - 選取要隱藏的警示類型。
   - 選取 [隱藏資訊警示]，隱藏所有資訊警示。
7 按一下 [確定]。

第 19 章

設定防火牆保護

防火牆提供一些方法，讓您管理安全性，以及設計您想要回應安全性事件及警示的方式。

第一次安裝防火牆之後，您的保護層級會設爲 [標準] 安全性。對大多數人而言，這個設定符合其所有安全性需求。但是，防火牆還提供其他層級，其範圍從完全限制到完全允許。

防火牆也讓您有機會接收有關警示及程式之網際網路存取權的建議。

在本章中

管理防火牆安全性層級

您可以設定安全性層級，以控制當防火牆偵測到無用的網路流量以及入埠及出埠的網際網路連線時，要管理及回應警示的程度。依預設，會啓用 [標準] 安全性層級。

當設定 [標準] 安全性層級並啓用 [自動建議] 時，紅色警示會提供選項，讓您授予或封鎖不明或已修改程式的存取權。當偵測到已知的程式時，綠色資訊警示即會出現，並自動授予存取權。授予存取權可讓程式建立出埠連線，並監聽來路不明的連入連線。

通常，安全性層級越嚴格 (如 [秘密] 及 [嚴密])，所顯示且必須由您處理的選項數及警示數就越多。

防火牆使用六種安全性層級。從最嚴格到最寬鬆，這些層級依序爲：

- **鎖定**：封鎖所有網際網路連線。
- **秘密**：封鎖所有入埠的網際網路連線。
- **嚴密**：警示要求您必須對每個入埠及出埠的網際網路連線要求做出回應。
- **標準**：警示會在不明或新程式需要存取網際網路時通知您。
- **信任**：授予所有入埠及出埠的網際網路連線存取權，並且自動將它們新增至 [程式權限] 窗格。
- **開放**：授予所有入埠及出埠網際網路連線的存取權。

防火牆也可讓您從 [還原防火牆保護預設值] 窗格立即將安全性層級重設爲標準。

將安全性層級設爲 [鎖定]

將防火牆的安全性層級設爲 [鎖定] 會封鎖所有入埠與出埠網路連線，包括網站、電子郵件及安全性更新的存取。這個安全性層級的效果相當於移除您的網際網路連線。您可以使用這個設定，來封鎖您在 [系統服務] 窗格上設定爲開放的通訊埠。在 [鎖定] 期間，警示會繼續提示您封鎖程式。

若要將防火牆的安全性層級設爲 [鎖定]：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。

2 在 [安全性等級] 窗格上移動滑桿，讓 [鎖定] 顯示爲目前的層級。

3 按一下 [確定]。

將安全性層級設為 [秘密]

將防火牆的安全性層級設為 [秘密] 會封鎖所有入埠網路連線 (但開放的通訊埠除外)。這個設定會完全隱藏您的電腦在網際網路上的存在。當安全性層級設為 [秘密] 時，防火牆會在新程式嘗試進行出埠網際網路連線或接收入埠連線要求時警示您。封鎖的和新增的程式都會出現在 [程式權限] 窗格上。

若要將防火牆的安全性層級設為 [秘密]：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [安全性等級] 窗格上移動滑桿，讓 [秘密] 顯示為目前的層級。
3 按一下 [確定]。

將安全性層級設為 [嚴密]

當安全性層級設為 [嚴密] 時，防火牆會在新程式嘗試進行出埠網際網路連線或接收入埠連線要求時通知您。封鎖的和新增的程式都會出現在 [程式權限] 窗格上。當安全性層級設為 [嚴密] 時，程式只會要求當時所需的存取權類型，例如限出埠存取權，您可以授予或封鎖此存取權。稍後，如果程式同時需要入埠及出埠連線，您可以從 [程式權限] 窗格將完整存取權授予程式。

若要將防火牆的安全性層級設為 [嚴密]：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [安全性等級] 窗格上移動滑桿，讓 [嚴密] 顯示為目前的層級。
3 按一下 [確定]。

將安全性層級設為 [標準]

[標準] 是預設且建議使用的安全性層級。

當防火牆的安全性層級設為 [標準] 時，防火牆會監視入埠及出埠連線，並在新程式嘗試存取網際網路時警示您。封鎖的和新增的程式都會出現在 [程式權限] 窗格上。

若要將防火牆的安全性層級設為 [標準]：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [安全性等級] 窗格上移動滑桿，讓 [標準] 顯示為目前的層級。
3 按一下 [確定]。

將安全性層級設為 [信任]

將防火牆的安全性層級設為 [信任] 會允許所有入埠及出埠連線。在 [信任] 安全性中，防火牆會自動將存取權授予所有程式，並將它們新增至 [程式權限] 窗格上允許的程式清單。

若要將防火牆的安全性層級設為 [信任]：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [安全性等級] 窗格上移動滑桿，讓 [信任] 顯示為目前的層級。
3. 按一下 [確定]。

設定警示的自動建議

您可以將防火牆設為在警示中包含、排除或顯示有關嘗試存取網際網路之程式的建議。

啟用 [自動建議] 可協助您決定如何處理警示。當啟用 [自動建議] (且安全性層級為 [標準]) 時，防火牆會自動授予或封鎖已知程式的存取權，並在偵測到未知及可能有危險的程式時，向您發出警示並建議一連串動作。

停用 [自動建議] 時，防火牆既不會自動授予或封鎖網際網路存取權，也不會建議一連串動作。

當防火牆設定為僅顯示 [自動建議] 時，會有一個警示提示您授予或封鎖存取權，但不過是建議一連串動作。

啟用自動建議

啟用 [自動建議] 可協助您決定如何處理警示。當 [自動建議] 啟用時，防火牆會自動授予或封鎖程式存取權，並警示您有關無法辨識及可能有危險的程式。

若要啟用 [自動建議]：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [安全性等級] 窗格的 [自動建議] 下，選取 [啟用自動建議]。
3 按一下 [確定]。

停用自動建議

當停用 [自動建議] 時，警示會排除有關處理警示及管理程式存取權的協助。如果停用 [自動建議]，防火牆會繼續授予及封鎖程式存取權，並警示您有關無法辨識及可能有危險的程式。此外，如果它偵測到可疑或是已知可能是威脅的新程式，防火牆會自動封鎖程式存取網際網路。

若要停用 [自動建議]：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [安全性等級] 窗格的 [自動建議] 下，選取 [停用自動建議]。
3 按一下 [確定]。

僅顯示自動建議

顯示 [自動建議] 可以協助您決定如何處理有關無法辨識及可能有危險之程式的警示。當 [自動建議] 設爲 [僅供顯示] 時，即會顯示有關如何處理警示的資訊，但是不同於 [啓用自動建議] 選項，它並不會自動套用所顯示的建議，而且也不會自動授予或封鎖程式存取權。相反的，警示只會提供建議，以協助您決定要授予或封鎖程式存取權。

若要僅顯示 [自動建議]：

1. 從 [網際網路與網路設定] 窗格中，按一下 [進階]。
2. 在 [安全性等級] 窗格的 [自動建議] 下，選取 [僅供顯示]。
3. 按一下 [確定]。

最佳化防火牆安全性

有許多可能會危及電腦安全性的方式。例如，有些程式會嘗試在 Windows® 啟動之前連線至網際網路。此外，經驗老道的電腦使用者可以 Ping 您的電腦，以判斷它是否已連線至網路。防火牆可讓您藉由啟用開機時間保護及封鎖 ICMP Ping 要求，應付這兩種類型的入侵。第一個設定會在 Windows 啟動時封鎖程式，使其無法存取網際網路，而第二個設定則會封鎖 Ping 要求，因為這種要求可協助其他使用者偵測您的電腦是否在網路上。

標準安裝設定包含自動偵測最常見的入侵嘗試，如拒絕服務攻擊或漏洞攻擊。使用標準安裝設定可確保免於這些攻擊及掃描的威脅；不過您可在 [入侵偵測] 窗格中停用一或多種攻擊或掃描的自動偵測。

啟動期間保護您的電腦

防火牆可以在 Windows 啟動時保護您的電腦。開機時間保護會封鎖所有先前未授予存取權且要求存取網際網路的新程式。在啟動防火牆之後，它會針對在啟動期間要求存取網際網路的程式顯示相關警示，您可以授予或封鎖其存取權。若要使用這個選項，您的安全性層級不得設為 [開放] 或 [鎖定]。

若要在啟動期間保護您的電腦：

1. 從 [網際網路與網路設定] 窗格中，按一下 [進階]。
2. 在 [安全性等級] 窗格的 [安全性設定] 下，選取 [啟用開機時間保護]。
3. 按一下 [確定]。

注意：啟用開機時間保護時，不會記錄已封鎖的連線及入侵。

設定 Ping 要求設定

電腦使用者可以使用傳送及接收 ICMP 回應要求訊息的 Ping 工具，來判斷指定的電腦是否已連線至網路。您可以設定防火牆，以防止或允許電腦使用者 Ping 您的電腦。

若要設定您的 ICMP Ping 要求設定：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [安全性等級] 窗格的 [安全性設定] 下，執行下列其中一項動作：
   - 選取 [允許 ICMP Ping 要求]，允許使用 Ping 要求以偵測您的電腦是否在網路上。
   - 清除 [允許 ICMP Ping 要求]，防止使用 Ping 要求來偵測您的電腦是否在網路上。

3 按一下 [確定]。

設定入侵偵測

入侵偵測 (IDS) 會監視資料封包中是否有可疑的資料傳輸或傳輸方法。IDS 會分析流量及資料封包，以尋找攻擊者所使用的特定流量模式。例如，如果防火牆測到 ICMP 封包，它會將 ICMP 流量與已知的攻擊模式進行比較，以分析這些封包是否有可疑的流量模式。防火牆會將封包與簽章資料庫進行比較，並且如果發現封包可疑或有害，就會捨棄來自攻擊電腦的封包，然後選擇性地記錄事件。

標準安裝設定包含自動偵測最常見的入侵嘗試，如拒絕服務攻擊或漏洞攻擊。使用標準安裝設定可確保免於這些攻擊及掃描的威脅；不過您可在 [入侵偵測] 窗格中停用一或多種攻擊或掃描的自動偵測。

若要設定入侵偵測：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。

2 在 [防火牆] 窗格上，按一下 [入侵偵測]。

3 在 [偵測入侵嘗試] 下，執行下列其中一項動作：

- 選取名稱以自動偵測攻擊或掃描。
- 清除名稱以停用自動偵測攻擊或掃描。

4 按一下 [確定]。

設定防火牆保護狀態設定

如果某些問題是整體電腦保護狀態一部份，SecurityCenter 就會追蹤它們。但是，您可以設定防火牆，忽略電腦上可能會影響保護狀態的特定問題。您可以設定 SecurityCenter，在防火牆設為 [開放] 安全性層級時、在防火牆服務不在執行時，或是限出埠防火牆未安裝在電腦上時略過這些問題。

若要設定 [防火牆保護狀態] 設定：

1 在 [常見工作] 窗格上，按一下 [進階功能表]。

2 按一下 [設定]。

3 在 [SecurityCenter 設定] 窗格上，按一下 [警示]。

4 按一下 [進階]。

5 在 [常見工作] 窗格上，按一下 [進階功能表]。

6 按一下 [設定]。

7 在 [SecurityCenter 設定] 窗格上，按一下 [保護狀態]。

8 按一下 [進階]。

9 在 [略過的問題] 窗格中，選取下列一個或多個選項：

- **防火牆的安全性層級已設為 [開放]。**

- 防火牆服務未執行。
- 出埠防火牆未安裝在您的電腦上。

10 按一下 [確定]。

鎖定及還原防火牆

鎖定功能在處理與電腦相關的緊急情況時非常有用，例如，當使用者必須封鎖所有流量以隔離自己的電腦並進行問題之疑難排解的時候，或是當使用者不確定、但是又必須決定如何管理程式存取網際網路的時候。

立即鎖定防火牆

鎖定防火牆會立即封鎖電腦和網際網路之間所有入埠和出埠的網路流量。並停止所有存取您電腦的遠端連線，且會封鎖電腦上的所有程式，使其無法存取網際網路。

若要立即鎖定防火牆並封鎖所有網路流量：

1 在已啓用 [基本功能表] 或 [進階功能表] 的 [首頁] 或 [常見工作] 上，按一下 [鎖定防火牆]。

2 在 [鎖定防火牆] 窗格上，按一下 [鎖定]。

3 在對話方塊上，按一下 [是]，以確認要立即封鎖所有入埠及出埠流量。

立即解除鎖定防火牆

鎖定防火牆會立即封鎖電腦和網際網路之間所有入埠和出埠的網路流量。並停止所有存取您電腦的遠端連線，且會封鎖電腦上的所有程式，使其無法存取網際網路。在鎖定防火牆之後，您可以解除鎖定以允許網路流量。

若要立即解除鎖定防火牆並允許網路流量：

1 在已啓用 [基本功能表] 或 [進階功能表] 的 [首頁] 或 [常見工作] 上，按一下 [鎖定防火牆]。

2 在 [啓用鎖定] 窗格上，按一下 [解除鎖定]。

3 在對話方塊上，按一下 [是]，以確認要解除鎖定防火牆並允許網路流量。

還原防火牆設定

您可以迅速地將防火牆還原爲原始保護設定。這樣會將安全性層級設爲 [標準]、啓用 [自動建議]、重設信任的和禁止的 IP 位址，並從 [程式權限] 窗格中移除所有程式。

若要將防火牆還原爲原始設定：

1. 在已啓用 [基本功能表] 或 [進階功能表] 的 [首頁] 或 [常見工作] 上，按一下 [還原防火牆預設值]。
2. 在 [還原防火牆保護預設值] 窗格上，按一下 [還原預設值]。
3. 在 [還原防火牆保護預設值] 對話方塊上，按一下 [是]，以確認要將防火牆還原爲預設值。

將安全性層級設爲 [開放]

將防火牆的安全性層級設爲 [開放] 會允許防火牆授予所有入埠及出埠網路連線的存取權。若要將存取權授予先前已封鎖的程式，請使用 [程式權限] 窗格。

若要將防火牆的安全性層級設爲 [開放]：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [安全性等級] 窗格上移動滑桿，讓 [開放] 顯示爲目前的層級。
3. 按一下 [確定]。

注意：當防火牆安全性層級設定爲 [開放] 時，之前已封鎖的程式仍將繼續封鎖。若要避免這種情況，您可以將程式的規則變更爲 [完整存取]。

第 20 章

管理程式及權限

防火牆可讓您為需要入埠及出埠網際網路存取權的現有程式與新程式管理及建立存取權。防火牆可讓您將完整存取權或限出埠存取權授予程式。您也可以封鎖程式的存取權。

在本章中

將網際網路存取權授予程式

有些程式 (如網際網路瀏覽器) 需要存取網際網路，才能正常運作。

防火牆可讓您使用 [程式權限] 頁面：

- 將存取權授予程式
- 將限出埠存取權授予程式
- 封鎖程式的存取權

您可以從出埠事件及最近的事件記錄檔授予完整及限出埠存取權。

將完整存取權授予程式

您電腦上有許多程式需要網際網路的入埠及出埠存取權。Personal Firewall 包含自動允許完整存取的程式清單，但是您可以修改這些權限。

若要將完整網際網路存取權授予程式：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [程式權限]。
3. 在 [程式權限] 下，選取具有 [已封鎖] 或 [限出埠存取] 的程式。
4. 在 [動作] 下，按一下 [授予完整存取權]。
5. 按一下 [確定]。

將完整存取權授予新程式

您電腦上有許多程式需要網際網路的入埠及出埠存取權。防火牆包含自動允許完整存取的程式清單，但是您可以新增程式並變更其權限。

若要將完整網際網路存取權授予新程式：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [程式權限]。
3. 在 [程式權限] 下，按一下 [新增允許的程式]。
4. 在 [新增程式] 對話方塊上，瀏覽並選取您要新增的程式。
5. 按一下 [開啓]。
6. 按一下 [確定]。

   剛新增的程式會出現在 [程式權限] 下。

注意：如同現有的程式一樣，您可以選取剛新增的程式，然後在 [動作] 下，按一下 [封鎖存取權] 或 [授予限出埠存取權] 以變更該程式的權限。

從最近的事件記錄檔授予完整存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。您可以從最近的事件記錄檔選取一個程式，然後授予它完整網際網路存取權。

若要從最近的事件記錄檔將完整存取權授予程式：

1. 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，選取事件說明，然後按一下 [授予完整存取權]。
3. 在 [程式權限] 對話方塊中，按一下 [是]，以確認要將完整存取權授予程式。

相關主題

- 檢視出埠事件 (第 153 頁)

從出埠事件記錄檔授予完整存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。您可以從出埠事件記錄檔選取一個程式，然後授予它完整的網際網路存取權。

若要從出埠事件記錄檔將完整網際網路存取權授予程式：

1. 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 選擇 [網際網路與網路]，然後再選擇 [出埠事件]。
4. 在 [出埠事件] 窗格中，選取來源 IP 位址，然後按一下 [授予存取權]。
5. 在 [程式權限] 對話方塊上，按一下 [是]，以確認要將完整網際網路存取權授予程式。

相關主題

- 檢視出埠事件 (第 153 頁)

將限出埠存取權授予程式

您電腦上有些程式只需要網際網路的出埠存取權。防火牆可讓您將網際網路的限出埠存取權授予程式。

將限出埠存取權授予程式

您電腦上有許多程式需要網際網路的入埠及出埠存取權。Personal Firewall 包含自動允許完整存取的程式清單，但是您可以修改這些權限。

若要授予程式僅限出埠存取權：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。

2 在 [防火牆] 窗格上，按一下 [程式權限]。

3 在 [程式權限] 下，選取具有 [已封鎖] 或 [完整存取] 的程式。

4 在 [動作] 下，按一下 [授予限出埠存取權]。

5 按一下 [確定]。

從最近的事件記錄檔授予限出埠存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。您可以從最近的事件記錄檔選取一個程式，然後授予它限出埠網際網路存取權。

若要從最近的事件記錄檔將限出埠存取權授予程式：

1 在 [常見工作] 窗格上，按一下 [報告與記錄]。

2 在 [最近的事件] 下，選取事件說明，然後按一下 [授予限出埠存取權]。

3 在 [程式權限] 對話方塊中，按一下 [是]，以確認要將限出埠存取權授予程式。

相關主題

- 檢視出埠事件 (第 153 頁)

從出埠事件記錄檔授予限出埠存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。您可以從出埠事件記錄檔選取一個程式，然後授予它限出埠網際網路存取權。

若要從出埠事件記錄檔將限出埠存取權授予程式：

1. 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 選擇 [網際網路與網路]，然後再選擇 [出埠事件]。
4. 在 [出埠事件] 窗格中，選取來源 IP 位址，然後按一下 [授予限出埠存取權]。
5. 在 [程式權限] 對話方塊中，按一下 [是]，以確認要授予程式限出埠存取權。

相關主題

- 檢視出埠事件 (第 153 頁)

封鎖程式的網際網路存取權

防火牆可讓您封鎖程式，使其無法存取網際網路。請確保封鎖程式不會中斷您的網路連線或另一個需要存取網際網路才能正常運作的程式。

封鎖程式的存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。Personal Firewall 包含自動允許完整存取的程式清單，但是您可以封鎖這些權限。

若要封鎖程式的網際網路存取權：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [程式權限]。
3. 在 [程式權限] 下，選取具有 [完整存取] 或 [限出埠存取] 的程式。
4. 在 [動作] 下，按一下 [封鎖存取權]。
5. 按一下 [確定]。

封鎖新程式的存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。Personal Firewall 包含自動允許完整存取的程式清單，但是您可以新增程式，然後封鎖其網際網路存取權。

若要封鎖新程式的網際網路存取權：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格下，按一下 [程式權限]。
3. 在 [程式權限] 下，按一下 [新增封鎖的程式]。
4. 在 [新增程式] 對話方塊上，瀏覽並選取您要新增的程式。
5. 按一下 [開啓]。
6. 按一下 [確定]。

   剛新增的程式會出現在 [程式權限] 下。

注意：如同現有的程式一樣，您可以選取剛新增的程式，然後在 [動作] 下，按一下 [授予完整存取權] 或 [授予限出埠存取權] 以變更該程式的權限。

從最近的事件記錄檔封鎖存取權

您電腦上有許多程式需要網際網路的入埠及出埠存取權。但是，您也可以選擇從最近的事件記錄檔將程式封鎖，使其無法存取網際網路。

若要從最近的事件記錄檔封鎖程式的存取權：

1 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2 在 [最近的事件] 下，選取事件說明，然後按一下 [封鎖存取權]。
3 在 [程式權限] 對話方塊中，按一下 [是]，以確認要封鎖程式。

相關主題

- 檢視出埠事件 (第 153 頁)

移除程式的存取權

移除程式的程式權限之前，請確定沒有該權限並不會影響您的電腦功能或網路連線。

移除程式權限

您電腦上有許多程式需要網際網路的入埠及出埠存取權。Personal Firewall 包含自動允許完整存取的程式清單，但是您可以移除自動及手動新增的程式。

若要移除新程式的程式權限：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。

2 在 [防火牆] 窗格上，按一下 [程式權限]。

3 在 [程式權限] 下，選取一個程式。

4 在 [動作] 下，按一下 [刪除程式權限]。

5 按一下 [確定]。

即會從 [程式權限] 窗格移除程式。

注意：防火牆會藉由將某些動作變灰及停用動作，來防止您修改某些程式。

瞭解程式

如果不確定要套用哪一個程式權限，您可以在 McAfee 的 HackerWatch 網站上取得程式的相關資訊，來協助您判斷。

取得程式資訊

您電腦上有許多程式需要網際網路的入埠及出埠存取權。Personal Firewall 包含自動允許完整存取的程式清單，但是您可以修改這些權限。

防火牆可以協助您決定要授予或封鎖程式的網際網路存取權。請確定您已連線至網際網路，讓瀏覽器能夠成功啟動 McAfee 的 HackerWatch 網站，這個網站會提供有關程式、網際網路存取需求及安全性威脅的最新資訊。

若要取得程式資訊：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [程式權限]。
3. 在 [程式權限] 下，選取一個程式。
4. 在 [動作] 下，按一下 [深入瞭解]。

從出埠事件記錄檔取得程式資訊

Personal Firewall 可讓您取得出埠事件記錄檔中出現之程式的相關資訊。

取得程式的相關資訊之前，請確定您有網際網路連線及網際網路瀏覽器。

若要從出埠事件記錄檔取得程式資訊：

1. 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 選擇 [網際網路與網路]，然後再選擇 [出埠事件]。
4. 在 [出埠事件] 窗格上，選取來源 IP 位址，然後按一下 [深入瞭解]。

   您可以在 HackerWatch 網站檢視程式的相關資訊。HackerWatch 會提供有關程式、網際網路存取需求及安全性威脅的最新資訊。

相關主題

- 檢視出埠事件 (第 153 頁)

第 21 章

管理系統服務

若要正常運作，某些程式 (包括 Web 伺服器和檔案共用伺服器程式) 必須透過指定的系統服務通訊埠接受來自其他電腦之來路不明的連線。通常，防火牆會關閉這些系統服務通訊埠，因爲它們最有可能造成您系統的不安全。但是，若要接受來自遠端電腦的連線，就必須開放系統服務通訊埠。

這個清單列出常見服務的標準通訊埠。

- 檔案傳輸協定 (FTP) 通訊埠 20-21
- 郵件伺服器 (IMAP) 通訊埠 143
- 郵件伺服器 (POP3) 通訊埠 110
- 郵件伺服器 (SMTP) 通訊埠 25
- Microsoft 目錄伺服器 (MSFT DS) 通訊埠 445
- Microsoft SQL Server (MSFT SQL) 通訊埠 1433
- 遠端協助 / 終端機伺服器 (RDP) 通訊埠 3389
- 遠端程序呼叫 (RPC) 通訊埠 135
- 安全的 Web 伺服器 (HTTPS) 通訊埠 443
- 通用隨插即用 (UPNP) 通訊埠 5000
- Web 伺服器 (HTTP) 通訊埠 80
- Windows 檔案共用 (NETBIOS) 通訊埠 137-139

在本章中

設定系統服務通訊埠

若要允許遠端電腦存取您電腦上的服務，您必須指定要開放的服務及相關通訊埠。請只選取您確定必須開放的服務及通訊埠。很少會需要開放通訊埠。

允許存取現有的系統服務通訊埠

從 [系統服務] 窗格可以開啓或關閉現有的通訊埠，來允許或拒絕遠端電腦存取您電腦上的網路服務。開放的系統服務通訊埠會讓您的電腦容易遭受網際網路的安全性威脅，因此只應在需要時才開放通訊埠。

若要允許存取系統服務通訊埠：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [防火牆] 窗格上，按一下 [系統服務]。
3 在 [開放系統服務通訊埠] 下，選取要開放通訊埠的系統服務。
4 按一下 [確定]。

封鎖對現有系統服務通訊埠的存取

從 [系統服務] 窗格可以開啓或關閉現有的通訊埠，來允許或拒絕遠端電腦存取您電腦上的網路服務。開放的系統服務通訊埠會讓您的電腦容易遭受網際網路的安全性威脅，因此只應在需要時才開放通訊埠。

若要封鎖對系統服務通訊埠的存取：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [防火牆] 窗格下，按一下 [系統服務]。
3 在 [開放系統服務通訊埠] 下，清除系統服務以關閉通訊埠。
4 按一下 [確定]。

設定新的系統服務通訊埠

從 [系統服務] 窗格中，您可以新增系統服務通訊埠，然後您可以開放或關閉這個系統服務通訊埠，以允許或拒絕遠端電腦存取您電腦上的網路服務。開放的系統服務通訊埠會讓您的電腦容易遭受網際網路的安全性威脅，因此只應在需要時才開放通訊埠。

若要建立及設定新的系統服務通訊埠：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [防火牆] 窗格上，按一下 [系統服務]。
3 按一下 [新增]。
4 在 [新增通訊埠設定] 下，指定下列項目：
   - 程式名稱
   - 入埠 TCP/IP 通訊埠
   - 出埠 TCP/IP 通訊埠
   - 入埠 UDP 通訊埠
   - 出埠 UDP 通訊埠
5 (可選) 說明新設定。
6 按一下 [確定]。

   剛設定的系統服務通訊埠會出現在 [開放系統服務通訊埠] 下。

修改系統服務通訊埠

開放及關閉的通訊埠會允許及拒絕遠端電腦存取您電腦上的網路服務。從 [系統服務] 窗格中，您可以修改現有通訊埠的入埠及出埠資訊。如果輸入不正確的通訊埠資訊，系統服務會失敗。

若要修改系統服務通訊埠：

1 從 [網際網路與網路設定] 窗格中，按一下 [進階]。
2 在 [防火牆] 窗格上，按一下 [系統服務]。
3 選取系統服務，然後按一下 [編輯]。
4 在 [新增通訊埠設定] 下，指定下列項目：
   - 程式名稱
   - 入埠 TCP/IP 通訊埠
   - 出埠 TCP/IP 通訊埠
   - 入埠 UDP 通訊埠
   - 出埠 UDP 通訊埠

5 (可選) 說明已修改的設定。

6 按一下 [確定]。

已修改的系統服務通訊埠會出現在 [開放系統服務] 下。

移除系統服務通訊埠

開放或關閉的通訊埠會允許或拒絕遠端電腦存取您電腦上的網路服務。從 [系統服務] 窗格中，您可以移除現有的通訊埠及相關的系統服務。從 [系統服務] 窗格移除通訊埠及系統服務之後，遠端電腦將不再能夠存取您電腦上的網路服務。

若要移除系統服務通訊埠：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。

2 在 [防火牆] 窗格上，按一下 [系統服務]。

3 選取一個系統服務，然後按一下 [移除]。

4 在 [系統服務] 對話方塊上，按一下 [是]，以確認要刪除該系統服務。

該系統服務通訊埠不再出現於 [系統服務] 窗格中。

第 22 章

管理電腦連線

您可以根據網際網路通訊協定位址 (IP) 建立與遠端電腦相關的規則，以設定防火牆來管理電腦的特定遠端連線。您可以信任與信任的 IP 位址相關的電腦連線至您的電腦，並禁止不明、可疑或不信任的 IP 連線至您的電腦。

允許連線時，請確定您信任的電腦是安全的。如果您信任的電腦透過病毒或其他機制受到感染，則您的電腦就可能會受到感染。此外，McAfee 建議您使用防火牆及最新的防毒程式來保護您信任的電腦。防火牆不會針對 [信任的 IP 位址] 清單中的 IP 位址記錄其傳來的流量或產生事件警示。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因為 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

在本章中

信任電腦連線

您可以在 [信任的和禁止的 IP] 窗格的 [信任的 IP 位址] 下，新增、編輯及移除信任的 IP 位址。

[信任的和禁止的 IP] 窗格中的 [信任的 IP 位址] 清單，可讓您允許所有來自特定電腦的流量到達您的電腦。防火牆不會針對 [信任的 IP 位址] 清單中的 IP 位址記錄其傳來的流量或產生事件警示。

防火牆會信任清單上的任何檢查過的 IP 位址，且一定會允許來自信任的 IP 的流量通過任何通訊埠上的防火牆。防火牆不會記錄任何來自信任的 IP 位址的事件。防火牆不會篩選或分析與信任的 IP 位址相關的電腦和您的電腦之間的活動。

允許連線時，請確定您信任的電腦是安全的。如果您信任的電腦透過病毒或其他機制受到感染，則您的電腦就可能會受到感染。此外，McAfee 建議您使用防火牆及最新的防毒程式來保護您信任的電腦。

新增信任的電腦連線

您可以使用防火牆，新增信任的電腦連線及其相關的 IP 位址。

[信任的和禁止的 IP] 窗格中的 [信任的 IP 位址] 清單，可讓您允許所有來自特定電腦的流量到達您的電腦。防火牆不會針對 [信任的 IP 位址] 清單中的 IP 位址記錄其傳來的流量或產生事件警示。

與信任的 IP 位址關聯之電腦，隨時可以連線到您的電腦。新增、編輯或移除信任的 IP 位址前，請確認它是可安全進行通訊或可移除的 IP 位址。

若要新增信任的電腦連線：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
3. 在 [信任的和禁止的 IP] 窗格上，選取 [信任的 IP 位址]。
4. 按一下 [新增]。
5. 在 [新增信任的 IP 位址規則] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [自 IP 位址] 及 [至 IP 位址] 方塊中，輸入開始及結束 IP 位址。

6 (可選) 選擇 [規則到期日期]，然後輸入實施規則的天數。

7 (可選) 輸入規則的說明。

8 按一下 [確定]。

9 在 [新增信任的 IP 位址規則] 對話方塊中，按一下 [是]，以確認要新增信任的電腦連線。

剛新增的 IP 位址會出現在 [信任的 IP 位址] 下。

從入埠事件記錄檔新增信任的電腦

您可以從入埠事件記錄檔新增信任的電腦連線及其相關的 IP 位址。

與信任的 IP 位址關聯之電腦，隨時可以連線到您的電腦。新增、編輯或移除信任的 IP 位址前，請確認它是可安全進行通訊或可移除的 IP 位址。

若要從入埠事件記錄檔新增信任的電腦連線：

1 請確定已啓用 [進階功能表]。在 [常見工作] 窗格上，按一下 [報告與記錄]。

2 在 [最近的事件] 下，按一下 [檢視記錄檔]。

3 按一下 [網際網路與網路]，然後按一下 [入埠事件]。

4 在 [入埠事件] 窗格上，選取來源 IP 位址，然後按一下 [信任此位址]。

5 在 [新增信任的 IP 位址規則] 對話方塊中，按一下 [是]，以確認要信任 IP 位址。

剛新增的 IP 位址會出現在 [信任的 IP 位址] 下。

相關主題

- 事件記錄 (第 152 頁)

編輯信任的電腦連線

您可以使用防火牆，編輯信任的電腦連線及其相關的 IP 位址。

與信任的 IP 位址關聯之電腦，隨時可以連線到您的電腦。新增、編輯或移除信任的 IP 位址前，請確認它是可安全進行通訊或可移除的 IP 位址。

若要編輯信任的電腦連線：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
3 在 [信任的和禁止的 IP] 窗格上，選取 [信任的 IP 位址]。
4 選取 IP 位址，然後按一下 [編輯]。
5 在 [編輯信任的 IP 位址規則] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [自 IP 位址] 及 [至 IP 位址] 方塊中，輸入開始及結束 IP 位址。
6 (可選) 勾選 [規則到期日期]，然後輸入實施規則的天數。
7 (可選) 輸入規則的說明。
8 按一下 [確定]。

   已修改的 IP 位址會出現在 [信任的 IP 位址] 下。

移除信任的電腦連線

您可以使用防火牆，移除信任的電腦連線及其相關的 IP 位址。

與信任的 IP 位址關聯之電腦，隨時可以連線到您的電腦。新增、編輯或移除信任的 IP 位址前，請確認它是可安全進行通訊或可移除的 IP 位址。

若要移除信任的電腦連線：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
3 在 [信任的和禁止的 IP] 窗格上，選取 [信任的 IP 位址]。
4 選取 IP 位址，然後按一下 [移除]。
5 在 [信任的和禁止的 IP] 對話方塊中，按一下 [是]，以確認要移除 [信任的 IP 位址] 下的信任的 IP 位址。

禁止電腦連線

您可以在 [信任的和禁止的 IP] 窗格的 [禁止的 IP 位址] 下，新增、編輯及移除信任的 IP 位址。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因爲 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

新增禁止的電腦連線

您可以使用防火牆，新增禁止的電腦連線及其相關的 IP 位址。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因爲 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

若要新增禁止的電腦連線：

1. 在 [網際網路與網路設定] 窗格上，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
3. 在 [信任的和禁止的 IP] 窗格上，選取 [禁止的 IP 位址]。
4. 按一下 [新增]。
5. 在 [新增禁止的 IP 位址規則] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [自 IP 位址] 及 [至 IP 位址] 欄位中，輸入開始及結束 IP 位址。
6. (可選) 勾選 [規則到期日期]，然後輸入實施規則的天數。
7. (可選) 輸入規則的說明。
8. 按一下 [確定]。
9. 在 [新增禁止的 IP 位址規則] 對話方塊上，按一下[是]，以確認要新增禁止的電腦連線。

   剛新增的 IP 位址會出現在 [禁止的 IP 位址] 下。

編輯禁止的電腦連線

您可以使用防火牆，編輯禁止的電腦連線及其相關的 IP 位址。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因爲 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

若要編輯禁止的電腦連線：

1 從 [網際網路與網路設定] 窗格中，按一下 [進階]。
2 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
3 在 [信任的和禁止的 IP] 窗格上，選取 [禁止的 IP 位址]。
4 選取 IP 位址，然後按一下 [編輯]。
5 在 [新增信任的 IP 位址規則] 下，執行下列其中一項動作：
   - 選取 [單一 IP 位址]，然後輸入 IP 位址。
   - 選取 [IP 位址範圍]，然後在 [自 IP 位址] 及 [至 IP 位址] 欄位中，輸入開始及結束 IP 位址。
6 (可選) 勾選 [規則到期日期]，然後輸入實施規則的天數。
7 (可選) 輸入規則的說明。

   按一下 [確定]。已修改的 IP 位址會出現在 [禁止的 IP 位址] 下。

移除禁止的電腦連線

您可以使用防火牆，移除禁止的電腦連線及其相關的 IP 位址。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因爲 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

若要移除禁止的電腦連線：

1. 從 [網際網路與網路設定] 窗格中，按一下 [進階]。
2. 在 [防火牆] 窗格上，按一下 [信任的和禁止的 IP]。
3. 在 [信任的和禁止的 IP] 窗格上，選取 [禁止的 IP 位址]。
4. 選取 IP 位址，然後按一下 [移除]。
5. 在 [信任的和禁止的 IP] 對話方塊上，按一下 [是]，以確認要從 [禁止的 IP 位址] 移除 IP 位址。

從入埠事件記錄檔禁止電腦

您可以從入埠事件記錄檔禁止電腦連線及其相關的 IP 位址。

入埠事件記錄檔中出現的 IP 位址會遭到封鎖。因此，除非您的電腦使用故意開放的通訊埠，或除非您的電腦包含已授予網際網路存取權的程式，否則禁止某個位址不會新增任何其他保護。

只有在您有一個或多個故意開啓的通訊埠，並且您有理由相信必須封鎖某個 IP 位址使其無法存取開放的通訊埠時，才應將 IP 位址新增至 [禁止的 IP 位址]。

您可以使用列出了所有入埠網際網路流量之 IP 位址的 [入埠事件] 頁，針對您懷疑為可疑或不當之網際網路活動的來源，禁止其 IP 位址。

若要從入埠事件記錄檔禁止信任的電腦連線：

1. 請確定已啓用 [進階功能表]。在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入埠事件]。
4. 在 [入埠事件] 窗格中，選取來源 IP 位址，然後按一下 [禁止此位址]。
5. 在 [新增禁止的 IP 位址規則] 對話方塊上，按一下 [是]，以確認要禁止 IP 位址。

   剛新增的 IP 位址會出現在 [禁止的 IP 位址] 下。

相關主題

- 事件記錄 (第 152 頁)

從入侵偵測事件記錄檔禁止電腦

您可以從出埠事件記錄檔禁止電腦連線及其相關的 IP 位址。

將會禁止使用不明、可疑或非信任 IP 位址的電腦連線到您的電腦。

因為 Firewall 會封鎖所有無用的流量，通常就不需要禁止 IP 位址。您只需要在確定某個網際網路連線會造成特定威脅時，才禁止該 IP 位址。請確定不要封鎖重要的 IP 位址，如您的 DNS 伺服器或 DHCP 伺服器，或與 ISP 相關的其他伺服器。根據安全性設定而定，Firewall 在偵測到來自禁止電腦的事件時可能會警示您。

若要從入侵偵測事件記錄檔禁止電腦連線：

1 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3 按一下 [網際網路與網路]，然後按一下 [入侵偵測事件]。
4 在 [入侵偵測事件] 窗格中，選取來源 IP 位址，然後按一下 [禁止此位址]。
5 在 [新增禁止的 IP 位址規則] 對話方塊上，按一下 [是]，以確認要禁止 IP 位址。

   剛新增的 IP 位址會出現在 [禁止的 IP 位址] 下。

相關主題

- 事件記錄 (第 152 頁)

第　23　章

記錄、監視及分析

防火牆為網際網路事件及流量提供詳盡且簡單易讀的記錄、監視及分析。瞭解網際網路流量及事件可協助您管理網際網路連線。

在本章中

事件記錄

Firewall 可讓您指定是否要啓用或停用記錄，以及指定啓用後所要記錄的事件類型。事件記錄可讓您檢視最近的入埠及出埠事件。您也可以檢視偵測到的入侵事件。

設定事件記錄檔設定

若要追蹤防火牆事件及活動，您可以指定及設定要檢視的事件類型。

若要設定事件記錄：

1 在 [網際網路與網路設定] 窗格上，按一下 [進階]。

2 在 [防火牆] 窗格上，按一下 [事件記錄檔設定]。

3 在 [事件記錄檔設定] 窗格上，執行下列其中一項動作：
   - 選取 [記錄事件] 來啓用事件記錄。
   - 選取 [不要記錄事件] 來停用事件記錄。

4 在 [事件記錄檔設定] 下，指定要記錄的事件類型。事件類型包括：
   - ICMP Ping
   - 來自禁止的 IP 位址的流量
   - 系統服務通訊埠上的事件
   - 不明通訊埠上的事件
   - 入侵偵測 (IDS) 事件

5 若要防止記錄特定通訊埠的相關資訊，請選取 [請勿記錄下列通訊埠上的事件]，然後輸入以逗號隔開的通訊埠號碼，或以破折號表示的通訊埠範圍。例如，137-139, 445, 400-5000。

6 按一下 [確定]。

檢視最近的事件

如果已啓用記錄，您可以檢視最近的事件。[最近的事件] 窗格會顯示事件的日期及說明。[最近的事件] 窗格只會顯示已明確封鎖，無法存取網際網路之程式的活動。

若要檢視防火牆最近的事件：

- 在 [進階功能表] 的 [常見工作] 窗格下，按一下 [報告與記錄] 或 [檢視最近的事件]。或者，從 [基本功能表] 按一下 [常見工作] 窗格下的 [檢視最近的事件]。

檢視入埠事件

如果已啓用記錄，您可以檢視並排序入埠事件。

入埠事件記錄檔包括下列記錄類別：

- 日期及時間
- 來源 IP 位址
- 主機名稱
- 資訊及事件類型

若要檢視您的防火牆入埠事件：

1. 請確定已啓用 [進階功能表]。在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入埠事件]。

注意：您可以從入埠事件記錄檔信任、禁止及追蹤 IP 位址。

相關主題

- 從入埠事件記錄檔新增信任的電腦 (第 143 頁)
- 從入埠事件記錄檔禁止電腦 (第 148 頁)
- 從入埠事件記錄檔追蹤電腦 (第 157 頁)

檢視出埠事件

如果已啓用記錄，您可以檢視出埠事件。出埠事件包括嘗試進行出埠存取的程式名稱、事件的日期及時間，以及程式在您電腦上的位置。

若要檢視您的防火牆出埠事件：

1. 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 選擇 [網際網路與網路]，然後再選擇 [出埠事件]。

注意：您可以從出埠事件記錄檔將完整存取權及限出埠存取權授予程式。您也可以尋找程式的其他相關資訊。

相關主題

- 從出埠事件記錄檔授予完整存取權 (第 129 頁)
- 從出埠事件記錄檔授予限出埠存取權 (第 131 頁)
- 從出埠事件記錄檔取得程式資訊 (第 135 頁)

檢視入侵偵測事件

如果已啓用記錄，您可以檢視入埠事件。入侵偵測事件會顯示事件的日期與時間、來源 IP 及主機名稱。記錄檔也會說明事件的類型。

若要檢視您的入侵偵測事件：

1. 在 [常見工作] 窗格下，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入侵偵測事件]。

注意：您可以從入侵偵測事件記錄檔禁止及追蹤 IP 位址。

相關主題

- 從入侵偵測事件記錄檔禁止電腦 (第 149 頁)
- 從入侵偵測事件記錄檔追蹤電腦 (第 157 頁)

使用統計資料

防火牆會利用 McAfee 的 HackerWatch 安全性網站，提供您有關全球網際網路安全性事件及通訊埠活動的統計資料。

檢視全球安全性事件統計資料

HackerWatch 會追蹤全球的網際網路安全性事件，您可以從 SecurityCenter 檢視這些事件。追蹤的資訊會列出在過去 24 小時、7 天及 30 天內向 HackerWatch 報告的事故。

若要檢視全球安全性統計資料：

1. 確定已啟用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [HackerWatch]。
3. 檢視 [事件追蹤] 下的安全性事件統計資料。

檢視全球網際網路通訊埠活動

HackerWatch 會追蹤全球的網際網路安全性事件，您可以從 SecurityCenter 檢視這些事件。顯示的資訊包括過去七天內向 HackerWatch 報告的最重要事件通訊埠。通常，會顯示 HTTP、TCP 及 UDP 通訊埠資訊。

若要檢視全球的通訊埠活動：

1. 確定已啟用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [HackerWatch]。
3. 檢視 [最近的通訊埠活動] 下的最重要事件通訊埠事件。

追蹤網際網路流量

防火牆會提供一些追蹤網際網路流量的選項。這些選項可讓您追蹤網路電腦的地理位置、取得網域及網路資訊，以及從入埠事件及入侵偵測事件記錄檔追蹤電腦。

追蹤網路電腦的地理位置

您可以使用視覺追蹤器，利用正在連線或嘗試連線至您電腦之電腦的名稱或 IP 位址，找出該電腦的位置。您也可以使用視覺追蹤器存取網路及註冊資訊。執行視覺追蹤器會顯示世界地圖，顯示從來源電腦到您的電腦最有可能的資料傳送路徑。

若要找出電腦的位置：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。
2 在 [工具] 窗格上，按一下 [視覺追蹤器]。
3 輸入電腦的 IP 位址，然後按一下[追蹤]。
4 在 [視覺追蹤器] 下，選取 [病毒活動圖檢視]。

注意：您無法追蹤迴圈、私人或無效的 IP 位址事件。

取得電腦註冊資訊

您可以使用視覺追蹤，從 SecurityCenter 取得電腦的註冊資訊。這些資訊包括網域名稱、註冊者的名稱及位址，以及管理聯絡人。

若要取得電腦的網域資訊：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。
2 在 [工具] 窗格上，按一下 [視覺追蹤器]。
3 輸入電腦的 IP 位址，然後按一下[追蹤]。
4 在 [視覺追蹤器] 下，選取 [註冊者檢視]。

取得電腦網路資訊

您可以使用視覺追蹤，從 SecurityCenter 取得電腦的網路資訊。網路資訊包括網域所在網路的詳細資料。

若要取得電腦的網路資訊：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。
2 在 [工具] 窗格上，按一下 [視覺追蹤器]。
3 輸入電腦的 IP 位址，然後按一下[追蹤]。
4 在 [視覺追蹤器] 下，選取 [網路檢視]。

從入埠事件記錄檔追蹤電腦

從 [入埠事件] 窗格中，您可以追蹤在入埠事件記錄檔中出現的 IP 位址。

若要從入埠事件記錄檔追蹤電腦的 IP 位址：

1. 請確定已啓用 [進階功能表]。在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入埠事件]。
4. 在 [入埠事件] 窗格上，選取來源 IP 位址，然後按一下 [追蹤此位址]。
5. 在 [視覺追蹤器] 窗格上，按一下下列其中一項：
   - **病毒活動圖檢視**：使用選取的 IP 位址，找出電腦的位址。
   - **註冊者檢視**：使用選取的 IP 位址，尋找網域資訊。
   - **網路檢視**：使用選取的 IP 位址，尋找網路資訊。
6. 按一下 [完成]。

相關主題

- 追蹤網際網路流量 (第 156 頁)
- 檢視入埠事件 (第 153 頁)

從入侵偵測事件記錄檔追蹤電腦

從 [入侵偵測事件] 窗格中，您可以追蹤在入侵偵測事件記錄檔中出現的 IP 位址。

若要從入侵偵測事件記錄檔追蹤電腦的 IP 位址：

1. 在 [常見工作] 窗格上，按一下 [報告與記錄]。
2. 在 [最近的事件] 下，按一下 [檢視記錄檔]。
3. 按一下 [網際網路與網路]，然後按一下 [入侵偵測事件]。 在 [入侵偵測事件] 窗格中，選取來源 IP 位址，然後按一下 [追蹤此位址]。
4. 在 [視覺追蹤器] 窗格上，按一下下列其中一項：
   - **病毒活動圖檢視**：使用選取的 IP 位址，找出電腦的位址。
   - **註冊者檢視**：使用選取的 IP 位址，尋找網域資訊。
   - **網路檢視**：使用選取的 IP 位址，尋找網路資訊。

5 按一下 [完成]。

相關主題

- 追蹤網際網路流量 (第 156 頁)
- 記錄、監視及分析 (第 151 頁)

追蹤監視的 IP 位址

您可以追蹤監視的 IP 位址以取得地理檢視，它會顯示從來源電腦到您的電腦最有可能的資料傳送路徑。此外，您也可以取得有關 IP 位址的註冊及網路資訊。

若要監視程式頻寬使用率：

1. 確定已啓用 [進階功能表]，然後按一下 [工具]。
2. 在 [工具] 窗格上，按一下 [流量監視]。
3. 在 [流量監視] 下，按一下 [作用中的程式]。
4. 選取一個程式，然後選取在該程式名稱下出現的 IP 位址。
5. 在 [程式活動] 下，按一下 [追蹤此 IP]。
6. 在 [視覺追蹤器] 下，您可以檢視一個地圖，它會顯示從來源電腦到您的電腦最有可能的資料傳送路徑。此外，您也可以取得有關 IP 位址的註冊及網路資訊。

注意：若要檢視最新的統計資料，請按一下 [視覺追蹤器] 下的 [重新整理]。

相關主題

- 監視網際網路流量 (第 159 頁)

監視網際網路流量

防火牆提供一些監視網際網路流量的方法，包括：

- **流量分析圖**：顯示最近的入埠及出埠網際網路流量。
- **流量使用率圖**：顯示過去 24 小時期間使用最頻繁的程式所佔用的頻寬百分比。
- **作用中的程式**：顯示目前在您電腦上使用最多網路連線的程式，以及這些程式存取的 IP 位址。

關於流量分析圖

流量分析圖以數字和圖形來表示網際網路流量，包括入埠和出埠流量。此外，流量監視會顯示電腦上使用大量網路連線的程式及這些程式所存取的 IP 位址。

從 [流量分析] 窗格中，您可以檢視最近的入埠及出埠網際網路流量，目前、平均及最大傳輸率。您也可以檢視流量，包括自從啓動防火牆後的流量，以及本月及上個月的總流量。

[流量分析] 窗格會顯示您電腦上的即時網際網路活動，包括您電腦上最近入埠及出埠的網際網路流量及其速率，以及跨網際網路傳輸的位元組總數。

綠色實線表示連入流量的目前傳輸速率。綠色虛線表示連入流量的平均傳輸速率。如果目前傳輸速率與平均傳輸速率相等，則圖中將不顯示虛線；實線同時表示平均傳輸速率和目前傳輸速率。

紅色實線表示連出流量的目前傳輸速率。紅色虛線表示連出流量的平均傳輸速率。如果目前傳輸速率與平均傳輸速率相等，則圖中將不顯示虛線；實線同時表示平均傳輸速率和目前傳輸速率。

相關主題

- 分析入埠及出埠流量 (第 160 頁)

分析入埠及出埠流量

流量分析圖以數字和圖形來表示網際網路流量，包括入埠和出埠流量。此外，流量監視會顯示電腦上使用大量網路連線的程式及這些程式所存取的 IP 位址。

若要分析入埠及出埠流量：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [流量監視]。

3 在 [流量監視] 下，按一下 [流量分析]。

> 秘訣：若要檢視最新的統計資料，請按一下 [流量分析] 下的 [重新整理]。

相關主題

- 關於流量分析圖 (第 159 頁)

監視程式頻寬

您可以檢視圓餅圖，它會顯示過去 24 小時期間使用最頻繁的程式所佔用的大約頻寬百分比。圓餅圖提供程式使用頻寬的相對數量之視覺展示。

若要監視程式頻寬使用率：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [流量監視]。

3 在 [流量監視] 下，按一下 [流量使用率]。

> 秘訣：若要檢視最新的統計資料，請按一下 [流量使用率] 下的 [重新整理]。

監視程式活動

您可以檢視入埠及出埠程式活動，它會顯示遠端電腦連線及通訊埠。

若要監視程式頻寬使用率：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。

2 在 [工具] 窗格上，按一下 [流量監視]。

3 在 [流量監視] 下，按一下 [作用中的程式]。

4 您可以檢視下列資訊：

   - 程式活動圖：選取要顯示其活動圖的程式。
   - 監聽連線：選取程式名稱下的監聽項目。
   - 電腦連線：選取程式名稱、系統處理程序或服務下的 IP 位址。

注意：若要檢視最新的統計資料，請按一下 [作用中的程式] 下的 [重新整理]。

第 24 章

瞭解網際網路安全性

防火牆會利用 McAfee 的安全性網站 (HackerWatch)，提供有關程式及全球網際網路活動的最新資訊。HackerWatch 也會提供有關防火牆的 HTML 教學課程。

在本章中

啓動 HackerWatch 教學課程

若要瞭解防火牆，您可以從 SecurityCenter 存取 HackerWatch 教學課程。

若要啓動 HackerWatch 教學課程：

1 確定已啓用 [進階功能表]，然後按一下 [工具]。
2 在 [工具] 窗格上，按一下 [HackerWatch]。
3 在 [HackerWatch 資源] 下，按一下 [檢視教學課程]。

第　25　章

McAfee SpamKiller

SpamKiller 會篩選垃圾郵件和網路釣魚電子郵件，並提供下列功能。

使用者選項

- 篩選多個電子郵件帳戶
- 將聯絡人匯入朋友清單
- 建立自訂的篩選器，並向 McAfee 報告垃圾郵件以供分析
- 標示為垃圾郵件及標示為非垃圾郵件選項
- 多使用者支援 (Windows® XP 與 Vista™)

篩選

- 自動更新篩選器
- 建立自訂的電子郵件篩選器
- 多層核心篩選引擎
- 網路釣魚篩選

在本章中

功能

此版本的 SpamKiller 提供下列功能。

篩選

先進的篩選技術可以加強您的使用者體驗。

網路釣魚

網路釣魚功能會輕易識別及封鎖潛在的網路釣魚網站。

安裝

簡化安裝與設定。

介面

直覺式使用者介面，讓您的電腦免受垃圾郵件之害。

支援

免費即時訊息與電子郵件技術支援，提供輕鬆、迅速及確實的客戶服務。

垃圾郵件處理

處理垃圾郵件的選擇性設定。這可以讓您檢視可能未正確篩選的郵件。

支援的電子郵件程式

- 任何 POP3 電子郵件程式
- Outlook® 2000 或更高版本的 MAPI 支援
- 使用 POP3 或付費 MSN®/Hotmail® 的 Web 郵件篩選器支援

支援的電子郵件工具列

- Outlook Express 6.0 或更高版本
- Outlook 2000、XP、2003 或 2007
- Eudora® 6.0 或更高版本
- Thunderbird™ 1.5 或更高版本

支援的網路釣魚保護

任何 HTTP 相容的 Web 瀏覽器，包括：

- Internet Explorer
- Firefox®
- Netscape®

第 26 章

管理 Web 郵件帳戶

您可以新增 Web 郵件帳戶來篩選垃圾郵件、編輯 Web 郵件帳戶資訊，或當您不再想要篩選 Web 郵件帳戶時將其移除。

您也可以管理 Web 郵件篩選。例如，可以停用或啓用在您的 Web 郵件帳戶中進行電子郵件篩選、管理已篩選的郵件，以及檢視記錄檔。

在本章中

新增 Web 郵件帳戶

您可以新增下列類型的 Web 郵件帳戶，系統便能篩選其中的垃圾郵件。

- POP3 Web 郵件 (例如，Yahoo®)
- MSN/Hotmail (只有付費的版本才能得到完整的支援)

新增 POP3 或 MSN/Hotmail Web 郵件帳戶

新增電子郵件帳戶，以便篩選其中是否有垃圾郵件。

若要新增 POP3 或 MSN/Hotmail Web 郵件帳戶：

1 按一下 [進階功能表]上的 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 按一下 [垃圾郵件保護] 底下的 [進階]。

4 按一下 [垃圾郵件保護] 窗格上的 [Web 郵件帳戶]。

5 在 [Web 郵件帳戶] 窗格上，按一下 [新增]。

6 指定下列方塊中的 Web 郵件帳戶資訊：
   - **說明**：說明帳戶。您可以在這個方塊中輸入任何資訊。
   - **電子郵件地址**：指定此帳戶的電子郵件地址。
   - **帳戶類型**：指定電子郵件帳戶的類型。
   - **伺服器**：指定此帳戶的伺服器名稱。
   - **使用者名稱**：指定此帳戶的使用者名稱。
   - **密碼**：指定用於存取此帳戶的密碼。
   - **確認密碼**：確認密碼。

7 按一下 [下一步]。

8 在 [檢查選項] 底下執行下列作業之一，以決定 SpamKiller 何時檢查您帳戶中的垃圾郵件：
   - 在 [檢查間隔] 方塊中輸入值。

     SpamKiller 會以您指定的時間間隔 (分鐘數) 檢查此帳戶。如果輸入數字零，SpamKiller 只會在帳戶連接時檢查帳戶。
   - 選取 [啓動時檢查] 核取方塊。

     SpamKiller 會在您每次重新啓動電腦時檢查帳戶。如果您使用直接連線，請使用此選項。

9 如果是使用撥號連線，請在 [連線選項] 底下執行下列任一作業，以決定 SpamKiller 如何連接至網際網路：
   - 按一下 [永遠不撥號連線]。

SpamKiller 不會自動幫您撥號連線。您必須手動啓動撥號連線。

- 按一下 [沒有可用連線時撥號]。

  沒有可用的網際網路連線時，SpamKiller 會嘗試使用您指定的撥號連線連接。

- 按一下 [永遠使用指定連線撥號]。

  SpamKiller 會嘗試使用您指定的撥號連線連接。

- 按一下 [撥號此連線] 清單中任一個項目。

  這個項目指定 SpamKiller 嘗試連接的撥號連線。

- 按一下 [篩選完成後仍保持連線] 核取方塊。

  您的電腦會在篩選完成後，保持與網際網路連線。

10 按一下 [完成]。

修改 Web 郵件帳戶

您可以啓用或停用 Web 郵件帳戶，或編輯其資訊。例如，您可以變更電子郵件地址、帳戶說明、帳戶類型、密碼、SpamKiller 檢查帳戶中垃圾郵件的頻率，以及電腦連線至網際網路的方式。

編輯 POP3 或 MSN/Hotmail Web 郵件帳戶

您可以啓用或停用 Web 郵件帳戶，或者編輯帳戶的資訊。例如，變更電子郵件地址、帳戶說明、伺服器資訊、SpamKiller 檢查帳戶是否有垃圾郵件的頻率，以及您的電腦如何連線到網際網路。

若要修改 POP3 或 MSN/Hotmail Web 郵件帳戶：

1 按一下 [進階功能表]上的 [設定]。
2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。
3 按一下 [垃圾郵件保護] 底下的 [進階]。
4 按一下 [垃圾郵件保護] 窗格上的 [Web 郵件帳戶]。
5 選取您要修改的帳戶，再按一下 [編輯]。
6 編輯下列方塊中的帳戶資訊：
   - **說明**：說明帳戶。您可以在這個方塊中輸入任何資訊。
   - **電子郵件地址**：指定此帳戶的電子郵件地址。
   - **帳戶類型**：指定電子郵件帳戶的類型
   - **伺服器**：指定此帳戶的伺服器名稱。
   - **使用者名稱**：指定此帳戶的使用者名稱。
   - **密碼**：指定用於存取此帳戶的密碼。
   - **確認密碼**：確認密碼。
7 按一下 [下一步]。
8 在 [檢查選項] 底下執行下列作業之一，以決定 SpamKiller 何時檢查您帳戶中的垃圾郵件：
   - 在 [檢查間隔] 方塊中輸入值。

     SpamKiller 會以您指定的時間間隔 (分鐘數) 檢查此帳戶。如果輸入數字零，SpamKiller 只會在帳戶連接時檢查帳戶。
   - 選取 [啓動時檢查] 核取方塊。

     SpamKiller 會在您每次重新啓動電腦時檢查帳戶。如果您使用直接連線，請使用此選項。
9 如果是使用撥號連線，請在 [連線選項] 底下執行下列任一作業，以決定 SpamKiller 如何連接至網際網路：
   - 按一下 [永遠不撥號連線]。

SpamKiller 不會自動幫您撥號連線。您必須手動啓動撥號連線。

- 按一下 [沒有可用連線時撥號]。

  沒有可用的網際網路連線時，SpamKiller 會嘗試使用您指定的撥號連線連接。

- 按一下 [永遠使用指定連線撥號]。

  SpamKiller 會嘗試使用您指定的撥號連線連接。

- 按一下 [撥號此連線] 清單中任一個項目。

  這個項目指定 SpamKiller 嘗試連接的撥號連線。

- 按一下 [篩選完成後仍保持連線] 核取方塊。

  您的電腦會在篩選完成後，保持與網際網路連線。

10 按一下 [完成]。

移除 Web 郵件帳戶

您可以移除不再想要篩選的 Web 郵件帳戶。

移除 Web 郵件帳戶

如果不再想要篩選電子郵件帳戶，請將其移除。

若要移除 Web 郵件帳戶：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [Web 郵件帳戶]。
5 選擇您要移除的帳戶，然後按一下 [移除]。

管理 Web 郵件篩選

可以停用或啓用在您的 Web 郵件帳戶中進行電子郵件篩選、管理已篩選的郵件，以及檢視記錄檔。

啓用 Web 郵件篩選

您可以停用 Web 郵件篩選並防止篩選電子郵件。

停用 Web 郵件篩選：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。

3 在 [垃圾郵件保護] 下，按一下 [進階]。

4 在 [垃圾郵件保護] 窗格上，按一下 [Web 郵件帳戶]。

5 清除您要停用之帳戶旁邊的核取方塊。

6 按一下 [確定]。

啓用 Web 郵件篩選

如果已停用任何 Web 郵件帳戶，您可以將其重新啓用。

啓用 Web 郵件篩選：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。

3 在 [垃圾郵件保護] 下，按一下 [進階]。

4 在 [垃圾郵件保護] 窗格上，按一下 [Web 郵件帳戶]。

5 選擇您要啓用之帳戶旁邊的核取方塊。

6 按一下 [確定]。

管理 Web 郵件帳戶中已篩選的郵件

您可以檢視、複製或刪除您已在 Web 郵件帳戶中篩選的郵件。

檢視、複製或刪除 Web 郵件帳戶的已篩選郵件：

1 在 [進階功能表] 上，按一下 [報告與記錄]。

2 在 [報告與記錄] 窗格上，按一下 [已篩選的 Web 郵件]。

3 在 [已篩選的 Web 郵件] 窗格上，選擇您要檢視、複製或刪除的郵件。

4 在 [我要] 下，執行下列其中一項動作：

- 按一下 [複製]，將郵件複製至剪貼簿。

- 按一下 [刪除] 以刪除郵件。

檢視已篩選 Web 郵件的記錄檔

您可以檢視已篩選 Web 郵件的記錄檔。例如，您可以檢視電子郵件的篩選時間及收到該電子郵件的帳戶。

若要檢視已篩選 Web 郵件的記錄檔：

1 在 [進階功能表] 上，按一下 [報告與記錄]。

2 在 [報告與記錄] 窗格上，按一下 [最近的事件]。

3 在 [最近的事件] 窗格上，按一下 [檢視記錄檔]。

4 在左窗格上，展開 [電子郵件與即時訊息] 清單，然後按一下 [Web 郵件篩選事件]。

5 選擇您要檢視的記錄檔。

6 在 [詳細資料] 下，檢視記錄檔的相關資訊。

第　27　章

管理朋友

若要確定收到朋友寄送的所有郵件，請將他們的地址新增至朋友清單。您也可以新增網域、編輯或移除朋友，以及排定朋友清單的自動更新時間。

在本章中

瞭解如何管理朋友

本節說明如何管理朋友。

從 SpamKiller 工具列手動新增朋友

為了確保您會收到朋友的訊息，請將朋友的地址新增至您的朋友清單中。

如果您是使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird 電子郵件程式，可以從 SpamKiller 工具列新增朋友。

若要從 Outlook 新增朋友：

- 在您的電子郵件程式中選取一封郵件，再按一下 [新增朋友]。

若要從 Outlook Express、Windows Mail、Eudora 或 Thunderbird 新增朋友：

- 在您的電子郵件程式中選取一封郵件。然後按一下 [SpamKiller] 功能表上的 [新增朋友]。

手動新增朋友

若要確定收到朋友寄送的所有郵件，請將他們的地址新增至朋友清單。您也可以新增網域。

手動新增朋友：

1. 在 [進階功能表] 上，按一下 [設定]。
2. 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3. 在 [垃圾郵件保護] 下，按一下 [進階]。
4. 在 [垃圾郵件保護] 窗格上，按一下 [朋友]。
5. 在 [朋友] 窗格上，按一下 [新增]。
6. 在下列方塊中，鍵入朋友的資訊：
   - **名稱**：指定朋友的名稱。
   - **類型**：指定您要指定單一電子郵件地址還是整個網域。
   - **電子郵件地址**：指定朋友的電子郵件地址，或您不想要篩選的網域。
7. 按一下 [確定]。

編輯朋友

如果朋友的資訊變更，您可以更新清單，以確保收到他們的所有郵件。

編輯朋友：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [朋友]。
5 選擇您要編輯的朋友，然後按一下 [編輯]。
6 在下列方塊中，編輯朋友的資訊：
   - **名稱**：指定朋友的名稱。
   - **類型**：指定您要編輯單一電子郵件地址還是整個網域。
   - **電子郵件地址**：指定朋友的電子郵件地址，或您不想要篩選的網域。
7 按一下 [確定]。

移除朋友

當您想要篩選朋友時，請從此清單移除他們。

若要移除朋友：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [朋友]。
5 選擇您要移除的朋友，然後按一下 [移除]。

自動更新朋友

若要確定收到朋友寄送的所有郵件，您可以從通訊錄手動匯入其地址，或排定自動更新時間。

手動匯入通訊錄

SpamKiller 可以匯入您的通訊錄並更新您的朋友。

手動匯入通訊錄：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [通訊錄]。
5 選擇要匯入的通訊錄，然後按一下 [立即執行]。
6 按一下 [確定]。

新增通訊錄

若要收到朋友寄送的所有郵件，請確定匯入時已包括通訊錄。

新增通訊錄：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [通訊錄]。
5 在 [通訊錄] 窗格上，按一下 [新增]。
6 在 [類型] 清單中，按一下您要匯入的通訊錄類型。
7 如果適用的話，請在 [來源] 清單中選擇通訊錄來源。
8 在 [排程] 清單中，按一下 [每日]、[每週] 或 [每月]，以決定 SpamKiller 檢查通訊錄以找出新地址的時間。
9 按一下 [確定]。

編輯通訊錄

SpamKiller 可以在指定的間隔匯入您的通訊錄並更新您的朋友。您也可以編輯通訊錄並變更通訊錄的匯入排程。

編輯通訊錄：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [通訊錄]。
5 選擇您要編輯的通訊錄，然後按一下 [編輯]。
6 請執行下列任一項動作：
   - 在 [類型] 清單中，按一下您要匯入的通訊錄類型。
   - 如果適用的話，請在 [來源] 清單中選擇通訊錄來源。
   - 在 [排程] 清單中，按一下 [每日]、[每週] 或 [每月]，以決定 SpamKiller 檢查通訊錄以找出新地址的時間。
7 按一下 [確定]。

移除通訊錄

當不再想要從通訊錄自動匯入地址時，請移除通訊錄。

若要移除通訊錄，不再自動匯入地址：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [通訊錄]。
5 選擇您要移除的通訊錄，然後按一下 [移除]。

第 28 章

修改篩選選項

篩選選項包括變更篩選層級、修改特殊篩選器、自訂郵件的處理方式、指定要篩選的字元集，以及向 McAfee 通報垃圾郵件。

在本章中

修改電子郵件篩選

您可以變更您要篩選郵件的積極程度。如果合法的電子郵件正被篩選掉，您可以降低篩選層級。

您也可以啓用或停用特殊篩選器。例如，依預設會篩選包含內容大多爲影像的郵件。如果想要收到這些郵件，您可以停用此篩選器。

變更電子郵件篩選層級

您可以變更您要篩選郵件的積極程度。例如，如果合法的電子郵件正被篩選掉，您可以降低篩選層級。

變更電子郵件篩選層級：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [篩選選項]。
5 在 [篩選選項] 下，將滑桿移至下列其中一項設定：
    - **低度**：接受大部分的電子郵件。
    - **中低度**：只篩選明顯的垃圾郵件。
    - **中度**：接受較多的電子郵件。
    - **中高度**：篩選任何類似垃圾郵件的電子郵件。
    - **高度**：只接受來自朋友清單中寄件者的郵件。
6 按一下 [確定]。

修改特殊篩選器

您可以啓用或停用特殊篩選器。例如，依預設會篩選包含內容大多爲影像的郵件。如果想要收到這些郵件，您可以停用此篩選器。

修改特殊篩選器：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 選擇 [篩選選項]。
5 在 [特殊篩選器] 下，啓用或停用下列任一個核取方塊：
    - **篩選包含隱藏文字的郵件**：隱藏文字是用來避開偵測。
    - **篩選內容中含有特定圖文比率的郵件**：所包含內容大多爲影像的郵件通常都是垃圾郵件。

- **篩選故意包含 HTML 格式錯誤的郵件**：無效格式化是用來防止篩選器篩選垃圾郵件。
- **不要篩選超過此大小的訊息**：不篩選大於指定大小的郵件。您可以增加或減少郵件大小 (有效範圍為 0-250 KB)。

6 按一下 [確定]。

修改郵件的處理方式

您可以變更垃圾郵件的標記或處理方式。例如，您可以變更垃圾郵件或網路釣魚標記的名稱，以及要將郵件留在收件匣，還是 SpamKiller 資料夾中。

修改郵件的處理方式

您可以變更垃圾郵件的標記或處理方式。例如，您可以變更垃圾郵件或網路釣魚標記的名稱，以及要將郵件留在收件匣，還是 SpamKiller 資料夾中。

修改 SpamKiller 處理垃圾郵件的方式：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [處理]。
5 執行下列其中一項：
   - 按一下 [標示為垃圾郵件並移到 SpamKiller 資料夾]。

     這是預設值。垃圾郵件會移到您的 SpamKiller 資料夾。
   - 按一下 [標示為垃圾郵件並留在收件匣中]。

     垃圾郵件仍會留在您的收件匣。
   - 在 [將這個可自訂的標記加到垃圾郵件的主旨中] 方塊中，鍵入自訂標記。

     您指定的標記會加到垃圾郵件的電子郵件主旨行。
   - 在 [將這個可自訂的標記加到網路釣魚郵件的主旨中] 方塊中，鍵入自訂標記。

     您指定的標記會加到網路釣魚郵件的電子郵件主旨行。
6 按一下 [確定]。

利用字元集篩選郵件

字元集用來表示語言，包括語言字母、數字及其他符號。您可以篩選包含特定字元集的郵件。然而，請不要篩選您接收的合法電子郵件所用語言的字元集。

例如，如果您想篩選義大利文郵件，但是想要接收合法的英文電子郵件，則請不要選取 [西歐語系]。選擇 [西歐語系] 不僅會篩選義大利文郵件，還會篩選英文郵件，以及西歐語系字元集中其他語言的郵件。

利用字元集篩選郵件

您可以篩選包含特定字元集的郵件。不過，請不要篩選您接收的合法電子郵件所用語言的字元集。

利用字元集篩選郵件：

1. 在 [進階功能表] 上，按一下 [設定]。
2. 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3. 在 [垃圾郵件保護] 下，按一下 [進階]。
4. 在 [垃圾郵件保護] 窗格上，按一下 [字元集]。
5. 選擇您要篩選之字元集旁邊的核取方塊。
6. 按一下 [確定]。

通報垃圾郵件

您可以向 McAfee 通報垃圾郵件，McAfee 會進行分析以建立篩選器更新。

通報垃圾郵件

您可以向 McAfee 通報垃圾郵件，McAfee 會進行分析以建立篩選器更新。

向 McAfee 報告垃圾郵件：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。

3 在 [垃圾郵件保護] 下，按一下 [進階]。

4 在 [垃圾郵件保護] 窗格上，按一下 [向 McAfee 通報]。

5 請選取下列其中一個核取方塊：

- **按一下 [標示為垃圾郵件] 時啟用通報**：會在每次將郵件標示為垃圾郵件時，向 McAfee 通報。
- **按一下 [標示為非垃圾郵件] 時啟用通報**：會在每次將郵件標示為非垃圾郵件時，向 McAfee 通報。
- **傳送整份郵件 (不僅標題)**：向 McAfee 通報郵件時，會傳送整份郵件，而不是只傳送標題。

6 按一下 [確定]。

第 29 章

管理個人篩選器

篩選器指定 SpamKiller 在電子郵件中尋找的內容。

SpamKiller 使用許多篩選器；不過，您可以建立新篩選器或編輯現有的篩選器，以微調將郵件識別爲垃圾郵件的標準。例如，如果篩選器運算式包含 "mortgage"，SpamKiller 會尋找包含 "mortgage" 這個字的郵件。

新增篩選器時，請仔細檢查您打算篩選的片語。如果片語在一般電子郵件中經常出現，請不要使用該片語。

在本章中

瞭解個人篩選器的管理方式

本節說明個人篩選器的管理方式。

新增個人篩選器

建立篩選器是選擇性的，而且會影響連入的電子郵件。因此，請勿建立可能在非垃圾郵件中出現之常見字的篩選器。

若要新增篩選器：

1 按一下 [進階功能表]上的 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 按一下 [垃圾郵件保護] 底下的 [進階]。

4 按一下 [垃圾郵件保護] 窗格上的 [個人篩選器]。

5 按一下 [新增]。

6 按一下 [項目] 清單中的一個項目，以決定篩選會在郵件主旨、內文、標題或郵件寄件者中尋找字或片語。

7 按一下 [條件] 清單中的一個項目，以決定篩選是要尋找包含 (或不包含) 您指定之字或片語的電子郵件。

8 在 [字或片語] 方塊中，輸入要在郵件中尋找的內容。例如，如果您指定 "mortgage"，將會篩選包含此字的所有郵件。

9 選取 [此篩選器使用規則運算式 (RegEx)] 核取方塊，以指定篩選條件中使用的字元模式。若要測試字元模式，請按一下 [測試]。

10 按一下 [確定]。

編輯個人篩選器

篩選器指定 SpamKiller 在電子郵件中尋找的內容。SpamKiller 使用許多篩選器；不過，您可以建立新篩選器或編輯現有的篩選器，以微調將郵件識別爲垃圾郵件的標準。

若要編輯篩選器：

1 按一下 [進階功能表]上的 [設定]。
2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。
3 按一下 [垃圾郵件保護] 底下的 [進階]。
4 按一下 [垃圾郵件保護] 窗格上的 [個人篩選器]。
5 選取您要編輯的篩選器，然後按一下 [編輯]。
6 按一下 [項目] 清單中的一個項目，以決定篩選器會在郵件主旨、內文、標題或郵件寄件者中尋找字或片語。
7 按一下 [條件] 清單中的一個項目，以決定篩選器是要尋找包含(或不包含) 您指定之字或片語的電子郵件。
8 在 [字或片語] 方塊中，輸入要在郵件中尋找的內容。例如，如果您指定 "mortgage"，將會篩選包含此字的所有郵件。
9 選取 [此篩選器使用規則運算式 (RegEx)] 核取方塊，以指定篩選條件中使用的字元模式。若要測試字元模式，請按一下 [測試]。
10 按一下 [確定]。

移除個人篩選器

您可以移除不再想要使用的篩選器。當移除篩選器時，即會永久地移除該篩選器。

移除篩選器：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格上，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [個人篩選器]。
5 選擇您要移除的篩選器，然後按一下 [移除]。
6 按一下 [確定]。

使用規則運算式

規則運算式是可在定義運算式時使用的特殊字元及序列。例如：

- 規則運算式 [0-9]*\.[0-9]+

  符合給定之非工程標記的浮點數。此規則運算式符合："12.12"、".1212" 及 "12.0"，但不符合 "12" 及 "12"。

- 規則運算式 \D*[0-9]+\D*

  符合所有具有數字的單字：SpamKi11er 及 V1AGRA，但 SpamKiller 及 VIAGRA 不算。

使用規則運算式

規則運算式是可在定義運算式時使用的特殊字元及序列。

\

將下一個字元標示爲特殊字元或文字。例如，n 符合字元 n。\n 符合換行字元。序列 \\ 符合 \，而 \(則符合 (。

^

符合輸入的開頭。

$

符合輸入的結尾。

*

符合前面字元零或多次。例如，zo* 符合 z 或 zoo。

+

符合前面字元一或多次。例如，zo+ 符合 zoo，但不符合 z。

?

符合前面字元零或一次。例如，a?ve? 符合 never 中的 ve。

.

符合任何單一字元，但換行字元除外。

(模式)

符合模式並記住符合項目。符合的子字串可以使用項目 [0]...[n]，從產生的符合集合中擷取。若要符合括弧字元 ( )，請使用 \(或 \)。

x|y

符合 x 或 y。例如，z|wood 符合 z 或 wood。(z|w)oo 符合 zoo 或 wood。

{n}

n 是非負數的整數。確切符合 n 次。例如，o{2} 不符合 Bob 中的 o，但符合 foooood 中的前兩個 o。

{n,}

n 是非負數的整數。至少符合 n 次。例如，o{2} 不符合 Bob 中的 o，但符合 foooood 中的所有 o。o{1,} 相當於 o+。o{0,} 相當於 o*。

{n,m}

m 及 n 皆是非負數的整數。至少符合 n 次且至多符合 m 次。例如，o{1,3} 符合 fooooood 中的前三個 o。o{0,1} 相當於 o?。

[xyz]

字元集。符合其中任何一個含括的字元。例如，[abc] 符合 plain 中的 a。

[^xyz]

否定字元集。符合任何未含括的字元。例如，[^abc] 符合 plain 中的 p。

[a-z]

字元範圍。符合指定範圍中的任何字元。例如，[a-z] 符合範圍 a 到 z 及 A 到 Z 中的任何小寫或大寫字母字元。

[A-Z]

字元範圍。符合指定範圍中的任何字元。例如，[A-Z] 符合範圍 A 到 Z 及 a 到 z 中的任何大寫或小寫字母字元。

[^m-z]

否定範圍字元。符合任何不在指定範圍內的字元。例如，[^m-z] 符合任何不在範圍 m 到 z 的字元。

\b

符合單字界限，也就是單字與空格之間的位置。例如，er\b 符合 never 中的 er，但不符合 verb 中的 er。

\B

符合非單字界限。ea*r\B 符合 never early 中的 ear。

\d

符合數字字元。相當於 [0-9]。

\D

符合非數字字元。相當於 [^0-9]。

\f

符合換頁字元。

\n

符合換行字元。

\r

符合回車字元。

\s

符合任何空白，包括空格、定位字元、換頁字元等。相當於 [\f\n\r\t\v]。

\S

符合任何非空白字元。相當於 [^ \f\n\r\t\v]。

\t

符合定位字元。

\v

符合垂直定位字元。

\w

符合任何單字字元，包括底線。相當於 [A-Za-z0-9_]。

\W

符合任何非單字字元。相當於 [^A-Za-z0-9_]。

\num

符合 num，其中 num 是正整數。重新參照記住的符合項目。例如，(.)\1 符合兩個連續的相同字元。\n 符合 n，其中 n 是八進位逸出值。八進位逸出值的長度必須是 1、2 或 3 個數字。例如，\11 及 \011 皆符合定位字元。\0011 相當於 \001 & 1。八進位逸出值不得超過 256。如果超過，只有前兩個數字構成運算式。允許在規則運算式中使用 ASCII 碼。

\xn

符合 n，其中 n 是十六進位逸出值。十六進位逸出值的長度必須是正好兩個數字。例如，\x41 符合 A。\x041 相當於 \x04 & 1。允許在規則運算式中使用 ASCII 碼。

第 30 章

維護 SpamKiller

維護 SpamKiller 的工作包括管理垃圾郵件保護及使用工具列。

管理垃圾郵件保護時，您可以停用或啟用篩選。

使用工具列時，您可以停用或啟用 SpamKiller 所提供的電子郵件工具列，以及從工具列將郵件標示爲垃圾郵件或非垃圾郵件。

在本章中

管理垃圾郵件保護

您可以停用或啓用電子郵件篩選。

停用垃圾郵件保護以防止篩選電子郵件，或啓用垃圾郵件保護以篩選電子郵件。

停用垃圾郵件保護

您可以停用垃圾郵件保護以防止篩選電子郵件。

停用篩選：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 在 [垃圾郵件保護] 下，按一下 [關閉]。

啓用垃圾郵件保護

您可以啓用垃圾郵件保護並篩選電子郵件。

啓用篩選：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。

3 在 [垃圾郵件保護] 下，按一下 [開啓]。

使用工具列

您可以針對支援的電子郵件用戶端停用或啓用電子郵件工具列。

如果您是使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird 電子郵件程式，也可以從 SpamKiller 工具列，將郵件標示爲垃圾郵件或非垃圾郵件。

停用工具列

您可以停用支援的電子郵件用戶端的工具列。

停用工具列：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [電子郵件工具列]，然後清除您要停用之工具列旁邊的核取方塊。
5 按一下 [確定]。

啓用工具列

任何工具列停用後，您都可以再次加以啓用。

啓用工具列：

1 在 [進階功能表] 上，按一下 [設定]。
2 在 [設定] 窗格中，按一下 [電子郵件與即時訊息]。
3 在 [垃圾郵件保護] 下，按一下 [進階]。
4 在 [垃圾郵件保護] 窗格上，按一下 [電子郵件工具列]，然後選擇您要啓用之工具列旁邊的核取方塊。
5 按一下 [確定]。

從 SpamKiller 工具列將電子郵件標示為垃圾郵件或非垃圾郵件

如果您是使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird 電子郵件程式，可以從 SpamKiller 工具列，將郵件標示為垃圾郵件或非垃圾郵件。

您將郵件標示為垃圾郵件時，郵件會貼上 [SPAM] 或您選擇的標籤，並保留在您的收件匣、SpamKiller 資料夾 (Outlook、Outlook Express、Windows Mail、Thunderbird) 或您的垃圾資料夾 (Eudora) 裡。

您將郵件標示為非垃圾郵件時，會移除郵件標籤，並將郵件移至您的收件匣。

若要從 Outlook 將郵件標示為垃圾郵件或非垃圾郵件：

1 在您的電子郵件程式中選取一封郵件。

2 在 [SpamKiller] 工具列上，按一下 [標示為垃圾郵件] 或 [標示為非垃圾郵件]。

若要從 Outlook Express、Windows Mail、Eudora 或 Thunderbird 將郵件標示為垃圾郵件或非垃圾郵件：

1 在您的電子郵件程式中選取一封郵件。

2 在 [SpamKiller] 功能表上，按一下 [標示為垃圾郵件] 或 [標示為非垃圾郵件]。

第 31 章

設定網路釣魚保護

未經許可的電子郵件分類爲垃圾郵件 (請求您購物的電子郵件) 或網路釣魚 (請求您提供個人資訊給詐欺網站或可能爲詐欺網站的電子郵件)。

網路釣魚篩選器可以協助保護您，避開詐欺網站。如果瀏覽至已知或潛在的詐欺網站，系統會讓您重新導向 [網路釣魚篩選器] 頁面。

您可以停用或啓用網路釣魚保護，或修改篩選選項。

在本章中

停用或啓用網路釣魚保護

您可以停用或啓用網路釣魚保護。例如，當您在嘗試存取您信任卻遭到封鎖的網站時，請停用網路釣魚保護。

停用網路釣魚保護

當嘗試存取您信任卻遭到封鎖的網站時，請停用網路釣魚保護。

停用網路釣魚保護：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [網際網路與網路]。

3 在 [網路釣魚] 下，按一下 [關閉]。

啓用網路釣魚保護

啓用網路釣魚保護，以確保您已受到保護，可避開網路釣魚網站。

啓用網路釣魚保護：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [網際網路與網路]。

3 在 [網路釣魚] 下，按一下 [開啓]。

修改網路釣魚篩選

McAfee 用以下兩種方法，判斷網站是否為網路釣魚網站：將您正在檢視的網站與已知的詐欺網站清單做比對，或嘗試判斷您正在檢視的網站是否為詐欺網站。

修改網路釣魚篩選

McAfee 用兩種方法，判斷網站是否為網路釣魚網站。如需完整保護，請選擇這兩個選項。

變更網路釣魚選項：

1 在 [進階功能表] 上，按一下 [設定]。

2 在 [設定] 窗格中，按一下 [網際網路與網路]。

3 在 [網路釣魚] 下，按一下 [進階]。

4 啟用或停用下列任一個核取方塊：

- **啟用黑名單與白名單查閱，以偵測詐欺網站**：將您正在檢視的網站與已知的詐欺網站清單做比對。
- **啟用探索式以偵測詐欺網站**：嘗試判斷您正在檢視的網站是否為詐欺網站。

5 按一下 [確定]。

第　32　章

其他說明

本章說明常見問題。

在本章中

常見問題解答

本節提供最常見之問題的解答。

何謂 POP3、MSN/Hotmail 及 MAPI 帳戶？

SpamKiller 是設計來使用這些類型的電子郵件帳戶：POP3、POP3 Web 郵件、MSN/Hotmail 及 MAPI。它們之間有一些差異，這些差異會影響 SpamKiller 執行篩選的方式。

POP3

這是最常用的帳戶類型，而且是網際網路電子郵件的標準。如果您有 POP3 帳戶，SpamKiller 會直接連接到伺服器，而且您的電子郵件程式在篩選郵件之後，才會加以擷取。

POP3 Web 郵件

POP3 Web 郵件帳戶是 Web 型帳戶。篩選 POP3 Web 郵件帳戶類似於篩選 POP3 帳戶。

MSN/Hotmail

MSN/Hotmail 帳戶是 Web 型帳戶。篩選 MSN/Hotmail 帳戶類似於篩選 POP3 帳戶。

MAPI

MAPI 是 Microsoft 設計的系統，它支援許多郵件類型，包括網際網路電子郵件、傳真及 Exchange Server 郵件。基於這個理由，MAPI 通常會用於 Microsoft® Exchange Server 的公司環境中。不過，許多人使用 Microsoft Outlook 收發個人網際網路電子郵件。SpamKiller 可以存取 MAPI 帳戶，但是請注意下列事項：

- 正常情況下，直到您以電子郵件程式擷取郵件，才會執行篩選。
- SpamKiller 只會篩選您的預設收件匣及網際網路電子郵件。

何謂網路釣魚篩選器？

未經許可的電子郵件分類爲垃圾郵件 (請求您購物的電子郵件) 或網路釣魚 (請求您提供個人資訊給詐欺網站或可能爲詐欺網站的電子郵件)。

網路釣魚篩選器可以協助保護您，避開列入黑名單的網站 (已確認的網路釣魚或相關之詐欺網站)，或列入灰名單的網站 (包含一些危險內容或黑名單網站的連結)。

如果瀏覽至已知或潛在的詐欺網站，系統會讓您重新導向 [網路釣魚篩選器] 頁面。

McAfee 爲何使用 Cookie？

McAfee 網站使用稱爲 Cookie 的軟體標籤，在客戶再次造訪網站時識別客戶。Cookies 是放在您電腦硬碟中的檔案中的文字區塊。Cookie 是下次您再存取該網站時，識別您的身份用的。

McAfee 會使用 Cookie 來：

- 管理您的訂閱權限及權利
- 識別出您是再度造訪的使用者，讓您不必於每次造訪時都要重新註冊
- 幫助瞭解您的購買喜好，以及自訂能夠滿足您的需要的服務
- 提供您可能有興趣的資訊、產品及優惠

McAfee 也會要求您提供您的名字，以便個人化您的網站使用經驗。

McAfee 無法爲瀏覽器設定爲拒絕 Cookie 的使用者提供訂閱服務。它不會銷售、租用或共用任何外部機構所收集的資訊。

McAfee 允許廣告商在訪客的瀏覽器中設定 Cookie。它無法存取廣告商的 Cookie 中所含的資訊。

第 33 章

McAfee Privacy Service

Privacy Service 為您及您的家庭、個人資料與電腦提供進階的保護。它可協助您抵禦線上身份被竊、封鎖個人識別資訊的傳輸，並篩選可能的不當線上內容 (包括影像、廣告、快顯視窗及網路臭蟲)。同時提供進階的未成年保護，可讓成人監視、控制並記錄孩童的 Web 瀏覽習慣與密碼的安全儲存區域。

開始使用 Privacy Service 之前，請先熟悉一些最常用的功能。Privacy Service 說明中會提供有關設定和使用這些功能的詳細資料。

在本章中

功能

Privacy Service 提供了下列功能：

- Web 瀏覽保護
- 個人資訊保護
- 未成年保護
- 密碼儲存區

Web 瀏覽保護

Web 瀏覽保護可讓您封鎖電腦上的廣告、快顯視窗及 Web 錯誤。封鎖廣告和快顯視窗可防止大部分的廣告和快顯視窗在瀏覽器中出現。封鎖 Web 錯誤可防止網站追蹤您的線上活動，並將資訊傳送給未經授權的來源。結合廣告、快顯視窗與 Web 錯誤封鎖可增加安全性，並防止來路不明的內容破壞 Web 瀏覽。

個人資訊保護

個人資訊保護可讓您封鎖在網際網路上傳輸敏感及機密資訊 (例如，信用卡號碼、銀行帳戶號碼、地址等等)。

未成年保護

未成年保護可讓您設定內容分級，此功能可以限制使用者所能檢視的網站及內容；也可以設定網際網路時間限制，指定使用者存取網際網路的期間及使用時間。未成年保護還可讓您全面限制對特定網站的存取權，並依據年齡群組及關聯的關鍵字，授權或封鎖存取權。

密碼儲存區

密碼儲存庫是您個人密碼的安全儲存區域。它能讓你放心儲存密碼，沒有其他使用者 (甚至是 McAfee 管理員或系統管理員) 可以存取。

第　34　章

設定未成年保護

新增使用者之後，您可設定該使用者的未成年保護。未成年保護爲定義使用者內容分級群組、Cookie 封鎖等級與網際網路時間限制的設定。內容分級群組根據使用者的年齡群組來決定使用者可存取之網際網路內容與網站的種類。Cookie 封鎖等級會決定當使用者登入時，是否可讓網站讀取他們在電腦上設定的 Cookie。網際網路時間限制定義使用者可存取網際網路的天數和時間。

您亦可設定一些適用所有未成年使用者的全域未成年保護。例如，當未成年使用者瀏覽網際網路時，您可封鎖或允許某些網站，或封鎖顯示可能的不當影像。您也可以爲所有的使用者設定全域 Cookie 封鎖設定。然而，若個別使用者的 Cookie 封鎖等級與全域 Cookie 封鎖設定不同，則會以全域設定優先。

注意：您必須是管理員才可設定未成年保護。

在本章中

設定使用者的內容分級群組

使用者可以屬於下列其中一種內容分級群組：

- 幼兒
- 兒童
- 少年 (較小)
- 少年 (較大)
- 成人

內容的分級 (亦即，可用或封鎖) 是根據使用者所屬的群組。例如，某些網站可能因使用者屬於幼兒群組而封鎖，但卻可為屬於少年 (較大) 群組的使用者所存取。屬於成人群組的使用者可以存取所有內容。依預設，新的使用者會自動加入幼兒群組，所有可向他們提供的內容皆受到限制。

身為管理員，您可以設定使用者的內容分級群組，然後根據這些群組來封鎖或允許網站。若您要更嚴格地對使用者進行內容分級，您也可以阻止使用者瀏覽不包含於全域 [允許的網站] 清單中的任何網站。如需更多資訊，請參閱依據關鍵字封鎖網站 (第 220 頁)與允許網站 (第 221 頁)。

設定使用者的內容分級群組

使用者內容分級群組是一個年齡群組，決定使用者可用之網際網路內容與網站的種類。

若要設定使用者的內容分級群組：

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3. 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4. 在 [使用者] 窗格上，按一下 [未成年保護]。
5. 選取清單中的使用者名稱。
6. 在 [內容分級] 底下，按一下您要指定給使用者的年齡群組。然後，您可根據每個年齡群組進行內容分級，讓您封鎖對特定年齡或成熟度顯示不當內容。
7. 若要限制使用者瀏覽不包含於全域 [允許的網站] 清單中的網站，請選取 [將使用者限制在「允許的網站」清單中的網站] 核取方塊。
8. 按一下 [確定]。

設定使用者的 Cookie 封鎖等級

有些網站會在您的電腦中建立稱爲 Cookie 的小檔案，以監視您的個人喜好與 Web 瀏覽習慣。身爲管理員，您可對使用者指定下列其中一項 Cookie 封鎖等級：

- 接受所有 Cookie
- 拒絕所有 Cookie
- 提示使用者接受 Cookie

接受所有 Cookie 設定可讓網站在對應使用者登入時，讀取設定於您電腦上的 Cookie。拒絕所有 Cookie 設定能防止網站讀取 Cookie。提示使用者接受 Cookie 設定會在每次有網站企圖在您的電腦上設定 Cookie 時，提示使用者。之後，使用者可依每次的情況，個別決定是否要允許 Cookie。於使用者決定接受或拒絕特定網站的 Cookie 後，將不會再提示該網站的 Cookie。

注意：某些網站需要您啓用 Cookie 才能正常運作。

設定使用者的 Cookie 封鎖等級

有些網站會在您的電腦中建立稱爲 Cookie 的小檔案，以監視您的個人喜好與 Web 瀏覽習慣。您可以爲電腦上的每位使用者指定處理 Cookie 的方法。

若要設定使用者的 Cookie 封鎖等級：

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3. 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4. 在 [使用者] 窗格上，按一下 [未成年保護]。
5. 選取清單中的使用者名稱。
6. 在 [Cookie 封鎖] 底下，按下列其中一項：
   - **接受所有 Cookie**：此使用者檢視的所有網站都可讀取他們在您電腦上設定的 Cookie。
   - **拒絕所有 Cookie**：此使用者檢視的任何網站都不能讀取他們在您電腦上設定的 Cookie。
   - **提示使用者接受 Cookie**：當此使用者嘗試檢視網站時隨即顯示訊息，提示使用者允許或拒絕 Cookie。
7. 按一下 [確定]。

將網站新增至使用者接受 Cookie 清單中

如果您設定使用者的 Cookie 封鎖等級爲提示網站設定 Cookie 的權限，但又要永遠允許某些網站能設定 Cookie 而無需提示，則您可將這些網站新增至使用者的接受 Cookie 清單中。

若要將網站新增至使用者接受 Cookie 清單中：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 按一下 [Cookie 封鎖] 下的 [檢視清單]。
7 在 [接受 Cookie 網站] 下，於 [http://] 方塊中鍵入網站位址，然後按一下 [新增]。
8 按一下 [完成]。

修改使用者接受 Cookie 清單中的網站

如果網站位址變更或將其新增至使用者接受 Cookie 清單時輸入不正確，您可以修改它。

若要修改使用者接受 Cookie 清單中的網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 按一下 [Cookie 封鎖] 下的 [檢視清單]。
7 在 [接受 Cookie 網站] 下，按一下 [網站] 清單中的項目，於 [http://] 方塊中修改網站位址，然後按一下 [更新]。
8 按一下 [完成]。

將網站從使用者接受 Cookie 清單中移除

如果您錯誤地將網站新增至使用者接受 Cookie 清單中，則可以移除它。

若要將網站從使用者接受 Cookie 清單中移除：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 按一下 [Cookie 封鎖] 下的 [檢視清單]。
7 在 [接受 Cookie 網站] 下，按一下 [網站] 清單中的項目，然後按一下 [移除]。
8 於 [移除確認] 對話方塊中，按一下 [是]。
9 按一下 [完成]。

將網站新增至使用者拒絕 Cookie 清單中

如果您設定使用者的 Cookie 封鎖等級為提示網站設定 Cookie 的權限，但又要永遠防止某些網站設定 Cookie 而無需提示，則您可將這些網站新增至使用者的拒絕 Cookie 清單中。

若要將網站新增至使用者拒絕 Cookie 清單中：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 按一下 [Cookie 封鎖] 下的 [檢視清單]。
7 按一下 [拒絕 Cookie 網站]。
8 在 [拒絕 Cookie 網站] 下，於 [http://] 方塊中鍵入網站位址，然後按一下 [新增]。
9 按一下 [完成]。

修改使用者拒絕 Cookie 清單中的網站

如果網站位址變更或將其新增至使用者拒絕 Cookie 清單時輸入不正確，您可以修改它。

若要修改使用者拒絕 Cookie 清單中的網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 按一下 [Cookie 封鎖] 下的 [檢視清單]。
7 按一下 [拒絕 Cookie 網站]。
8 在 [拒絕 Cookie 網站] 下，按一下 [網站] 清單中的項目，於 [http://] 方塊中修改網站位址，然後按一下 [更新]。
9 按一下 [完成]。

將網站從使用者拒絕 Cookie 清單中移除

如果您錯誤地將網站新增至使用者拒絕 Cookie 清單中，則可以移除它。

若要將網站從使用者拒絕 Cookie 清單中移除：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 按一下 [Cookie 封鎖] 下的 [檢視清單]。
7 按一下 [拒絕 Cookie 網站]。
8 在 [拒絕 Cookie 網站] 下，按一下 [網站] 清單中的項目，然後按一下 [移除]。
9 於 [移除確認] 對話方塊中，按一下 [是]。
10 按一下 [完成]。

設定使用者的網際網路時間限制

身為管理員，如果當使用者可以存取網際網路時，您可使用網際網路時間限制格線來指定。您可授予使用者無限制的網際網路使用、受限制的網際網路使用，或完全禁止網際網路使用。

網際網路時間限制格線可讓您指定以三十分鐘為間隔的時間限制。格線的綠色部分表示使用者可存取網際網路的天數和時間。格線的紅色部分表示拒絕存取的天數和時間。如果使用者試圖於禁止期間存取網際網路，McAfee 會通知使用者不可以這麼做。

如果您禁止某位使用者存取整個網際網路，則該使用者可以登入並使用電腦，但無法使用網際網路。

設定使用者的網際網路時間限制

您可使用網際網路時間限制格線來指定特定使用者何時可以存取網際網路。格線的綠色部分表示使用者可存取網際網路的天數和時間。格線的紅色部分表示拒絕存取的天數和時間。

若要設定使用者的網際網路時間限制：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 資訊] 底下按一下 [設定]。
3 在 [SecurityCenter 設定] 窗格上，按一下 [使用者] 下的 [進階]。
4 在 [使用者] 窗格上，按一下 [未成年保護]。
5 選取清單中的使用者名稱。
6 在 [網際網路時間限制] 下，按住並拖曳以指定這位使用者可存取網際網路的天數和時間。
7 按一下 [確定]。

封鎖網站

如果您是管理員，且您要防止所有未成年使用者存取某特定網站，則您應封鎖該網站。當使用者嘗試存取封鎖的網站時，隨即會顯示訊息指出該網站無法存取，因爲已被 McAfee 所封鎖。

即使網站列於 [封鎖的網站] 清單中，屬於成人年齡群組的使用者 (包括管理員) 仍可存取所有網站。若要測試封鎖的網站，您必須以未成年使用者身份登入。

身爲管理員，您亦可依據網站上所包含的關鍵字來封鎖網站。McAfee 維持一份關鍵字與對應規則的預設清單，該清單能決定當某關鍵字存在時，是否允許某年齡群組使用者進行瀏覽。啓用關鍵字掃描時，會使用關鍵字的預設清單來問使用者進行內容分級。然而，您可將自己可允許的關鍵字新增至預設清單，並與某些年齡群組相關聯。您新增的關鍵字規則會取代與預設清單中相符合關鍵字相關聯的規則。您可以查閱現有的關鍵字或指定與特定年齡群組相關聯的新關鍵字。

封鎖網站

若您要防止所有未成年使用者存取該網站，則可以封鎖該網站。如果某位使用者嘗試存取該網站，隨即會顯示訊息指出該網站以遭 McAfee 封鎖。

若要封鎖網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，請確定已啓用 [未成年保護]，然後按一下 [進階]。
5 在 [封鎖的網站] 窗格上，於 [http://] 方塊中鍵入網站位址，然後按一下 [新增]。
6 按一下 [確定]。

修改封鎖的網站

如果網站位址變更或將其新增至 [封鎖的網站] 清單時輸入不正確，您可以修改它。

若要修改封鎖的網站：

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3. 於 [未成年保護] 資訊區段中，按一下 [設定]。
4. 在 [未成年保護設定] 窗格上，按一下 [進階]。
5. 在 [封鎖的網站] 窗格上，按一下 [封鎖的網站] 清單中的項目，於 [http://] 方塊中修改網站位址，然後按一下 [更新]。
6. 按一下 [確定]。

移除封鎖的網站

如果您不再封鎖網站，必須從 [封鎖的網站] 清單中移除。

若要移除封鎖的網站：

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3. 於 [未成年保護] 資訊區段中，按一下 [設定]。
4. 在 [未成年保護設定] 窗格上，按一下 [進階]。
5. 在 [封鎖的網站] 窗格上，按一下 [封鎖的網站] 清單中的項目，然後按一下 [移除]。
6. 於 [移除確認] 對話方塊中，按一下 [是]。
7. 按一下 [確定]。

停用關鍵字掃描

預設會啓用關鍵字掃描，即會使用 McAfee 預設的關鍵字清單為使用者進行內容分級。雖然 McAfee 並不建議您這麼做，但您可隨時停用關鍵字掃描。

若要停用關鍵字掃描：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [關鍵字掃描]。
6 在 [關鍵字掃描] 窗格上，按一下 [關閉]。
7 按一下 [確定]。

依關鍵字封鎖網站

如果您要依據內容來封鎖網站但卻不知道特定的網址，則可以依據其關鍵字來封鎖網站。只要輸入一個關鍵字，然後決定哪個年齡組可以及無法檢視包含該關鍵字的網站。

若要依關鍵字封鎖網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [關鍵字掃描] 並確定開啓。
6 在 [全域未成年保護] 窗格上，按一下 [關鍵字]。
7 於 [尋找] 方塊中鍵入一個關鍵字。
   包含這個字的網站將會遭到封鎖。
8 移動 [最小年齡] 滑桿以指定最小年齡群組。
   這個年齡群組及較高的使用者可以檢視包含關鍵字的網站。
9 按一下 [確定]。

允許網站

如果您是管理員，您可以讓所有使用者存取特定網站，覆寫任何預設值與封鎖的網站。

如需有關已封鎖網站的更多資訊，請參閱封鎖網站 (第 218 頁)。

允許網站

若您要確定某個網站並爲針對任何使用者而封鎖，您可將網站位址新增至 [允許的網站] 清單中。當您將網站新增至 [允許的網站] 清單時，您會覆寫任何預設值及已新增至 [封鎖的網站] 清單的網站。

若要允許網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [允許的網站]。
6 在 [允許的網站] 窗格上，於 [http://] 方塊中鍵入網站位址，然後按一下 [新增]。
7 按一下 [確定]。

秘訣：您可防止使用者瀏覽任何不在 [允許的網站] 清單中的網站。如需更多資訊，請參閱設定使用者的內容分級群組 (第 212 頁)。

修改允許的網站

如果網站位址變更或將其新增至 [允許的網站] 清單時輸入不正確，您可以修改它。

若要修改允許的網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [允許的網站]。
6 在 [允許的網站] 窗格上，按一下 [允許的網站] 清單中的項目，於 [http://] 方塊中修改位址，然後按一下 [更新]。
7 按一下 [確定]。

移除允許的網站

您可以隨時移除允許的網站。依據您的設定，當您從 [允許的網站] 清單移除網站時，McAfee 使用者可能無法再存取該網站。

若要移除允許的網站：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [允許的網站]。
6 在 [允許的網站] 窗格上，按一下 [允許的網站] 清單中的項目，然後按一下 [移除]。
7 於 [移除確認] 對話方塊中，按一下 [是]。
8 按一下 [確定]。

允許網站設定 Cookie

若您封鎖所有網站不能讀取他們在您電腦上設定的 Cookie，或設定某些使用者在接受 Cookie 之前接收訊息提示，之後發現該特定網站無法正常運作，您可以允許這些網站來讀取其 Cookie。

如需有關 Cookie 封鎖等級的更多資訊，請參閱設定使用者的 Cookie 封鎖等級 (第 213 頁)。

允許網站設定 Cookie

若您封鎖所有網站不能讀取他們在您電腦上設定的 Cookie，或設定某些使用者在接受 Cookie 之前接收訊息提示，之後發現該特定網站無法正常運作，您可以允許這些網站來讀取其 Cookie。

若要允許網站設定 Cookie：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [Cookie]。
6 在 [Cookies] 窗格上，於 [http://] 方塊中鍵入網站位址，然後按一下 [新增]。
7 按一下 [確定]。

修改接受 Cookie 清單

如果網站位址變更或將其新增至 [接受 Cookie] 清單時輸入不正確，您可以修改它。

若要修改 Cookie 清單：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [Cookie]。
6 在 [Cookie] 窗格上，按一下 [接受 Cookie] 清單中的項目，於 [http://] 方塊中修改位址，然後按一下 [更新]。
7 按一下 [確定]。

防止網站設定 Cookie

如果您要防止特定網頁讀取其在您電腦上設定的 Cookie，您可由 [接受 Cookie] 清單中將它移除。

若要防止網站設定 Cookie：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [Cookie]。
6 在 [Cookie] 窗格上，按一下 [接受 Cookie] 清單中的項目，然後按一下 [移除]。
7 於 [移除確認] 對話方塊中，按一下 [是]。
8 按一下 [確定]。

封鎖可能的不當 **Web** 影像

瀏覽網際網路時封鎖可能的不當影像使其無法顯示，以保護您的家庭成員。可針對所有使用者或成人年齡群組之外的所有使用者封鎖影像。如需有關年齡群組的更多資訊，請參閱設定使用者的內容分級群組 (第 212 頁)。

預設會針對成人年齡群組之外的所有使用者啓用影像分析；但身爲管理員，您可隨時停用它。

封鎖可能的不當影像

依預設，McAfee 會啓用影像分析，在瀏覽網際網路時封鎖可能的不當影像使其無法顯示，以保護您的家庭成員。如果 McAfee 偵測到一個可能的不當影像，它會以一個自訂的影像取代該影像，並指出原始影像已遭封鎖。您必須是管理員才能停用影像分析。

若要封鎖可能的不當影像：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格上，按一下 [未成年保護]。
3 於 [未成年保護] 資訊區段中，按一下 [設定]。
4 在 [未成年保護設定] 窗格上，按一下 [進階]。
5 在 [全域未成年保護] 窗格上，按一下 [影像分析]。
6 請在 [影像分析] 窗格上，執行下列其中一項動作：
    - 按一下 [所有使用者] 以對所有使用者封鎖可能的不當影像。
    - 按一下 [青少年與兒童] 以對所有使用者 (除了成人年齡群組成員外) 封鎖可能的不當影像。
7 按一下 [確定]。

第 35 章

保護網際網路上的資訊

當瀏覽網際網路時，請使用 Privacy Service 以保護您家人與個人資訊。例如，若您是管理員，當使用者在網際網路上時，您可以設定 McAfee 來封鎖廣告、快顯視窗及網路臭蟲。您也可以將您的個人資料 (例如，姓名、住址、信用卡號碼和銀行帳戶號碼) 新增至封鎖的資訊區域，以防止這些資料透過網路傳送。

在本章中

封鎖廣告、快顯視窗與網路臭蟲

若您是管理員，當使用者在網際網路上時，您可以設定 McAfee 來封鎖廣告、快顯視窗及網路臭蟲。封鎖廣告和快顯視窗可防止大部分的廣告和快顯式視窗在 Web 瀏覽器中出現。這可幫助增進您瀏覽網際網路的速度與效率。封鎖網路臭蟲可防止網站追蹤您的線上活動，並將資訊傳送給未經授權的來源。網路臭蟲 (亦稱為網站信標、像素標籤、透明影像圖檔，或看不見的影像圖檔) 是小的圖形檔案，它可以內嵌於您的 HTML 頁面，並允許未經授權的來源設定您電腦上的 Cookie。這些 Cookie 之後便可將資訊傳輸至未經授權的來源。

依預設，您的電腦會封鎖廣告、快顯視窗及網路臭蟲。身為管理員，您可以隨時允許廣告、快顯視窗及網路臭蟲。

封鎖廣告

您可以在使用者存取網際網路時封鎖廣告，使其無法顯示。

若要封鎖廣告：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。
3 於 [網際網路與網路] 資訊區段中，按一下 [設定]。
4 在 [網際網路與網路設定] 窗格上，按一下 [Web 瀏覽保護] 下的 [進階]。
5 在 [廣告、快顯視窗與網路臭蟲封鎖] 窗格上，選取 [當您瀏覽網際網路時，封鎖網頁上出現的廣告] 核取方塊。
6 按一下 [確定]。

封鎖快顯視窗

您可以在使用者存取網際網路時封鎖快顯視窗，使其無法顯示。

若要封鎖快顯視窗：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。
3 於 [網際網路與網路] 資訊區段中，按一下 [設定]。
4 在 [網際網路與網路設定] 窗格上，按一下 [Web 瀏覽保護] 下的 [進階]。
5 在 [廣告、快顯視窗與網路臭蟲封鎖] 窗格上，選取 [當您瀏覽網際網路時，封鎖快顯視窗，使其無法顯示] 核取方塊。
6 按一下 [確定]。

封鎖網路臭蟲

網路臭蟲 (亦稱爲網站信標、像素標籤、透明影像圖檔，或看不見的影像圖檔) 是小的圖形檔案，它可以內嵌於您的 HTML 頁面，並允許未經授權的來源設定您電腦上的 Cookie。這些 Cookie 之後便可將資訊傳輸至未經授權的來源。您可封鎖網路臭蟲以防止其載入至您的電腦上。

若要封鎖網路臭蟲：

1 按一下 [常見工作] 下的 [首頁]。

2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。

3 於 [網際網路與網路] 資訊區段中，按一下 [設定]。

4 在 [網際網路與網路設定] 窗格上，按一下 [Web 瀏覽保護] 下的 [進階]。

5 在 [廣告、快顯視窗與網路臭蟲封鎖] 窗格上，選取 [封鎖此電腦上的網路臭蟲] 核取方塊。

6 按一下 [確定]。

封鎖個人資訊

將您的個人資料 (例如，姓名、住址、信用卡號碼和銀行帳戶號碼) 新增至封鎖的資訊區域，以防止這些資料透過網路傳送。當 McAfee 偵測到個人識別資訊可能遭到送出，將發生以下狀況：

- 如果您是管理員，會出現提示要求您確認是否送出資訊。
- 如果您不是管理員，則封鎖的資訊將以星號 (*) 取代。例如，如果您傳送一封電子郵件 Lance Armstrong wins tour，而 Armstrong 被設定為要封鎖的個人資訊，則所傳送的電子郵件將變為 Lance ********* wins tour。

您可以封鎖以下類型的個人資訊：姓名、住址、郵遞區號、社會安全資訊、電話號碼、信用卡號碼、銀行帳戶、經紀帳戶與電話卡。如果您要封鎖不同類型的個人資訊，您可將類型設定為 [其他]。

封鎖個人資訊

您可以封鎖以下類型的個人資訊：姓名、住址、郵遞區號、社會安全資訊、電話號碼、信用卡號碼、銀行帳戶、經紀帳戶與電話卡。如果您要封鎖不同類型的個人資訊，您可將類型設定為 [其他]。

若要封鎖個人資訊：

1 按一下 [常見工作] 下的 [首頁]。

2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。

3 於 [網際網路與網路] 資訊區段中，按一下 [設定]。

4 在 [網際網路與網路設定] 窗格上，確定個人資訊保護已啓用，然後按一下 [進階]。

5 在 [封鎖的資訊] 窗格上，按一下 [新增]。

6 選擇清單中您要封鎖的資訊類型。

7 輸入您的個人資訊，然後按一下 [確定]。

8 於 [個人資訊保護] 對話方塊中，按一下 [確定]。

第 36 章

保護密碼

密碼儲存庫是您個人密碼的安全儲存區域。它能讓你放心儲存密碼，沒有其他使用者 (甚至是 McAfee 管理員或系統管理員) 可以存取。

在本章中

設定密碼儲存庫

開始使用密碼儲存庫之前，您必須設定密碼儲存庫密碼。只有知道這個密碼的使用者才可以存取您的密碼儲存庫。如果您忘記密碼儲存庫密碼，您可以重設；然而，所有先前曾儲存於您密碼儲存庫中的密碼將遭到刪除。

設定密碼儲存庫密碼後，您可以新增、編輯或移除您儲存庫中的密碼。

將密碼新增至密碼儲存庫

如果您有記憶密碼的問題，您可將其新增至密碼儲存庫。密碼儲存庫是一個安全的地方，只有知道您密碼儲存庫密碼的使用者才能進行存取。

若要將密碼新增至密碼儲存庫：

1. 按一下 [常見工作] 下的 [首頁]。
2. 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。
3. 於 [網際網路與網路] 資訊區段中，按一下 [設定]。
4. 在 [網際網路與網路設定] 窗格上，按一下 [個人資訊保護] 下的 [進階]。
5. 在 [個人資訊保護] 窗格上，按一下 [密碼儲存庫]。
6. 在 [密碼] 方塊中鍵入您密碼儲存庫的密碼，然後在 [確認密碼] 方塊中再鍵入一次。
7. 按一下 [開啓]。
8. 在 [密碼儲存庫] 窗格上，按一下 [新增]。
9. 在 [說明] 方塊中鍵入密碼的說明 (例如，其用途)，然後在 [密碼] 方塊中鍵入密碼。
10. 按一下 [新增]，然後按一下 [確定]。

修改密碼儲存庫中的密碼

爲確保您密碼儲存庫中的項目永遠準確且可靠，當密碼變更時，您必須更新他們。

若要修改密碼儲存庫中的密碼：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。
3 於 [網際網路與網路] 資訊區段中，按一下 [設定]。
4 在 [網際網路與網路設定] 窗格上，按一下 [個人資訊保護] 下的 [進階]。
5 在 [個人資訊保護] 窗格上，按一下 [密碼儲存庫]。
6 於 [密碼] 方塊中鍵入您的密碼儲存庫密碼。
7 按一下 [開啓]。
8 在 [密碼儲存庫] 窗格上，按一下密碼項目，然後按一下 [編輯]。
9 在 [說明] 方塊中修改密碼的說明 (例如，其用途)，或在 [密碼] 方塊中修改密碼。
10 按一下 [新增]，然後按一下 [確定]。

將密碼從密碼儲存庫中移除

您可隨時從密碼儲存庫中移除密碼。從儲存庫中移除密碼後便無法復原。

若要將密碼從密碼儲存庫中移除：

1 按一下 [常見工作] 下的 [首頁]。
2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。
3 於 [網際網路與網路] 資訊區段中，按一下 [設定]。
4 在 [網際網路與網路設定] 窗格上，按一下 [個人資訊保護] 下的 [進階]。
5 在 [個人資訊保護] 窗格上，按一下 [密碼儲存庫]。
6 於 [密碼] 方塊中鍵入您的密碼儲存庫密碼。
7 按一下 [開啓]。
8 在 [密碼儲存庫] 窗格上，按一下密碼項目，然後按一下 [移除]。
9 於 [移除確認] 對話方塊中，按一下 [是]。
10 按一下 [確定]。

重設密碼儲存庫密碼

如果您忘記密碼儲存庫密碼，您可以重設；然而，所有您先前輸入的密碼都將遭到刪除。

若要重設密碼儲存庫密碼：

1 按一下 [常見工作] 下的 [首頁]。

2 在 [SecurityCenter 首頁] 窗格中，按一下 [網際網路與網路]。

3 於 [網際網路與網路] 窗格中，按一下 [設定]。

4 在 [網際網路與網路設定] 窗格上，按一下 [個人資訊保護] 下的 [進階]。

5 在 [個人資訊保護] 窗格上，按一下 [密碼儲存庫]。

6 在 [重設密碼儲存庫] 下，於 [密碼] 方塊中鍵入新的密碼，然後在 [確認密碼] 方塊中再鍵入一次。

7 按一下 [重設]。

8 於 [重設密碼確認] 對話方塊中，按一下 [是]。

第 37 章

McAfee Data Backup

使用 Data Backup 將您的檔案封存至 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟中以避免您資料的意外遺失。本機封存可讓您將您的個人資料封存 (備份) 於 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟中。為防止意外遺失，這可為您的紀錄、文件，及其他個人興趣的資料提供本機副本。

開始使用 Data Backup 之前，請先熟悉一些最常用的功能。Data Backup 說明中會提供有關設定和使用這些功能的詳細資料。於瀏覽該程式功能之後，您必須確定具有可用的適當封存媒體以執行本機封存。

在本章中

功能

Data Backup 提供了下列功能，可以儲存與還原您的照片、音樂及其他重要的檔案。

本機排定封存

將您的檔案與資料夾封存至 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟機以保護您的資料。於您起始第一個封存後，將會自動進行遞增式封存。

單鍵還原

若檔案與資料夾在您的電腦上遭到錯誤地刪除或損毀，您可從用來封存的媒體還原最近的封存版本。

壓縮與加密

依預設會壓縮您的封存檔案，這可節省您封存媒體的空間。作為額外的安全性措施，你的封存依預設會進行加密。

第 38 章

封存檔案

您可使用 McAfee Data Backup，將您電腦上的檔案副本封存於 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟中。為防止意外的資料遺失或損壞，利用這個方法封存您的檔案可使您更易擷取資訊。

開始封存檔案前，您必須選擇您的預設封存位置 (CD、DVD、USB 磁碟機、外接硬碟或網路磁碟)。McAfee 已預先設定一些其他的設定；例如，您要封存的資料夾與檔案類型，但是您可以修改這些設定。

設定本機封存選項後，您可修改 Data Backup 執行完整或快速封存頻率的預設值。您可以隨時執行手動封存。

在本章中

設定封存選項

開始封存資料之前，您必須設定某些本機封存選項。例如，您必須設定觀察位置與觀察檔案類型。觀察位置是您電腦上的資料夾，可為 Data Backup 監視新的檔案或檔案變更。觀察檔案類型為 Data Backup 於觀察位置內進行封存的檔案類型 (例如，.doc、.xls 等等)。依預設，Data Backup 觀察儲存於您觀察位置中的所有檔案類型。

您可以設定兩種觀察位置類型：深層觀察位置與淺層觀察位置。如果您設定深層觀察位置，Data Backup 會於該資料夾及其子資料夾內封存觀察檔案類型。如果您設定淺層觀察位置，Data Backup 會僅於該資料夾 (非其子資料夾) 內封存觀察檔案類型。您亦可識別您要從本端封存排除的位置。依預設，將 Windows 桌面與「我的文件」位置設定為深層觀察位置。

設定您的觀察檔案類型與位置後，您必須設定封存位置 (亦即，儲存封存資料的 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟)。您可以隨時變更封存位置。

基於安全與大小理由，依預設對您的封存檔案啓用加密或壓縮。加密檔案的內容從文字轉換為代碼，掩飾資訊，使那些不知如何解密的人們無法讀取。將壓縮的檔案壓縮為最小化所需空間的格式以將之儲存或傳送。雖然 McAfee 並不建議您這麼做，但您可隨時停用加密或壓縮。

封存中包含位置

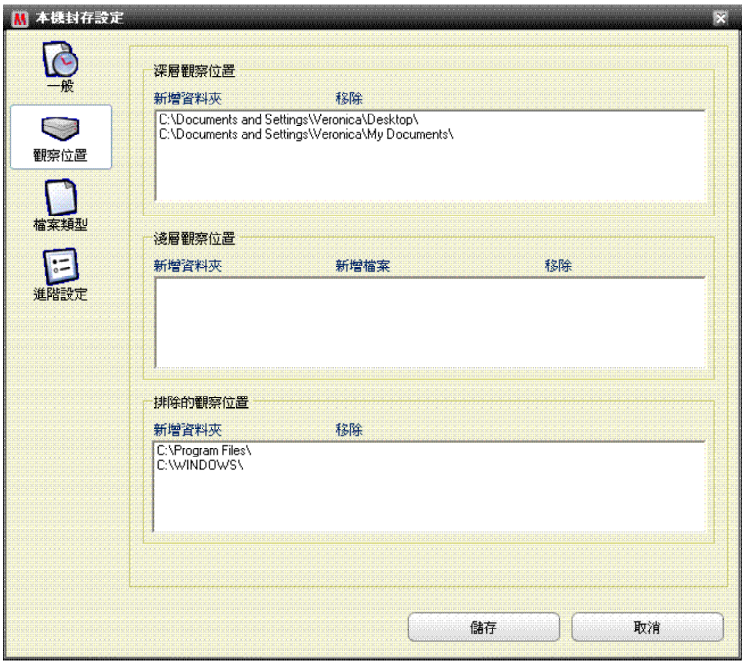
您可以設定兩種封存的觀察位置類型：深層觀察位置與淺層觀察位置。如果您設定深層觀察位置，Data Backup 會監視該資料夾及其子資料夾的內容變化。如果您設定淺層觀察位置，Data Backup 僅會監視資料夾 (非其子資料夾) 的內容。

若要於封存中包含位置：

1 按一下 [本機封存] 索引標籤。

2 於左窗格中，按一下 [設定]。

3 於 [本機封存設定] 對話方塊中，按一下 [觀察位置]。



4 執行下列其中一項：

- 若要封存某個資料夾的內容 (包含其子資料夾的內容)，按一下 [深層觀察位置] 下的 [新增資料夾]。
- 若要封存某個資料夾的內容 (但不包含其子資料夾的內容)，按一下 [淺層觀察位置] 下的 [新增資料夾]。

5 於 [瀏覽資料夾] 對話方塊中，導覽至您要觀察的資料夾，然後按一下 [確定]。

6 按一下 [儲存]。

秘訣：若您要 Data Backup 觀察您尚未建立的資料夾，您可按一下 [瀏覽資料夾] 對話方塊中的 [建立新資料夾] 以新增資料夾，同時將其設定為觀察位置。

設定封存檔案類型

您可指定哪些檔案類型可於您的深層或淺層觀察位置中封存。您可從現有的檔案類型清單選擇或將新類型新增至清單。

若要設定封存檔案類型：

1 按一下 [本機封存] 索引標籤。

2 於左窗格中，按一下 [設定]。

3 於 [本機封存設定] 對話方塊中，按一下 [檔案類型]。

4 展開檔案類型清單，選取您要封存檔案類型旁的核取方塊。

5 按一下 [儲存]。

秘訣：若要將新的檔案類型增加至 [選取的檔案類型] 清單中，請於 [將自訂檔案類型新增至 [其他]] 方塊中鍵入副檔名，然後按一下 [新增]。新的檔案類型自動成爲觀察檔案類型。

從封存排除位置

若您要防止某個位置 (資料夾) 及其內容在線上遭到封存，您可將該位置從封存排除。

若要從封存排除位置：

1 按一下 [本機封存] 索引標籤。

2 於左窗格中，按一下 [設定]。

3 於 [本機封存設定] 對話方塊中，按一下 [觀察資料夾]。

4 按一下 [排除的觀察位置] 下的 [新增資料夾]。

5 於 [瀏覽資料夾] 對話方塊中，導覽至您要排除的資料夾，將之選取，然後按一下 [確定]。

6 按一下 [儲存]。

秘訣：若您要 Data Backup 排除您尚未建立的資料夾，您可按一下 [瀏覽資料夾] 對話方塊中的 [建立新資料夾] 以新增資料夾，同時將其排除。

變更封存位置

變更封存位置時，先前封存於不同位置的檔案將列為 [從未封存]。

若要變更封存位置：

1 按一下 [本機封存] 索引標籤。

2 於左窗格中，按一下 [設定]。

3 按一下 [變更封存位置]。

4 於 [封存位置] 對話方塊中，執行下列任一項：

- 按一下 [選取 CD/DVD 寫入器]，按一下 [寫入器] 清單中您電腦的 CD 或 DVD 磁碟機，然後按一下 [儲存]。
- 按一下 [選取磁碟機位置]，導覽至 USB 磁碟機、本機磁碟，或外接硬碟，加以選取，然後按一下 [確定]。
- 按一下 [選取網路位置]，導覽至網路資料夾，加以選取，然後按一下 [確定]。

5 確認 [選取的封存位置] 下的新封存位置，然後按一下 [確定]。

6 於確認對話方塊中，按一下 [確定]。

7 按一下 [儲存]。

停用封存加密與壓縮

加密封存的檔案可保護您資料的機密性，防止檔案內容的洩露，因此無法讀取。壓縮的封存檔案可協助您最小化檔案大小。依預設，啓用加密與壓縮兩者；但是，您可以隨時停用這些選項。

若要停用封存加密與壓縮：

1 按一下 [本機封存] 索引標籤。

2 於左窗格中，按一下 [設定]。

3 於 [本機封存設定] 對話方塊中，按一下 [進階設定]。

4 清除 [啓用加密以增加安全性] 核取方塊。

5 清除 [啓用壓縮以減少儲存] 核取方塊。

6 按一下 [儲存]。

注意：McAfee 建議您當封存檔案時，不要停用加密與壓縮。

執行完整與快速的封存

您可以執行兩種封存類型：完整或快速。執行完整封存時，您封存一組根據您已設定之觀察檔案類型與位置的完整資料。執行快速封存時，您僅對那些自上次完整或快速封存後變更的觀察檔案進行封存。

依預設，排定 Data Backup 每星期一早上 9:00 於您的觀察位置執行觀察檔案類型的完整封存，而於前次的完整或快速封存後每 48 小時執行一次快速封存。此排程可確保隨時都在維護您檔案目前的封存。然而，如果您不要每 48 小時便進行一次封存，您可以視需要調整排程。

若您要於指定時才封存您觀察位置的內容，您可隨時這麼做。例如，若您修改某個檔案並要將其封存，但並未於未來的幾小時內排定 Data Backup 執行完整或快速封存，則您可以手動方式封存檔案。當您手動封存檔案時，您為自動封存所設定的時間間隔將重設。

若封存在不恰當的時間發生時，您亦可中斷自動或手動備份。例如，若您正在執行資源密集的工作，而自動封存卻開始了，您可以將自動封存停止。當您停止自動封存時，您為自動封存所設定的時間間隔將重設。

排定自動封存

您可以設定完整與快速封存的頻率，以確保您的資料永遠受到保護。

若要排定自動封存：

1 按一下 [本機封存] 索引標籤。

2 於左窗格中，按一下 [設定]。

3 於 [本機封存設定] 對話方塊中，按一下 [一般]。

4 若要每天、每週、或每個月執行一次完整封存，請按一下 [完整封存，每隔] 下的任一項：
   - 日
   - 週
   - 月

5 選取您要執行完整封存之日旁的核取方塊。

6 按一下 [於] 清單中的值，指出您要執行完整封存的時間。

7 若要每天或每小時執行一次快速封存，請按一下 [快速封存] 下的任一項：
   - 小時
   - 天

8 於 [快速封存，每隔] 方塊中鍵入表示頻率的數字。

9 按一下 [儲存]。

中斷自動封存

根據您所定義的排程，Data Backup 可於您觀察位置中自動封存檔案。然而，若自動封存正在進行中，而您要將其中斷，則您可隨時這麼做。

若要中斷自動封存：

1 於左窗格中，按一下 [停止封存]。

2 於確認對話方塊中，按一下 [是]。

注意：當封存正在進行中時，才會出現 [停止封存]。

手動執行封存

雖然自動封存是根據預先定義的排程，您可隨時以手動方式執行快速或完整封存。快速封存僅對那些自前次完整或快速封存後已變更的檔案進行封存。完整的封存會對所有觀察位置中的觀察檔案類型進行封存。

若要以手動方式執行快速或完整封存：

1 按一下 [本機封存] 索引標籤。

2 若要執行快速封存，按一下左窗格中的 [快速封存]。

3 若要執行完整封存，按一下左窗格中的 [完整封存]。

4 在 [準備開始封存] 對話方塊中，確認您的儲存空間與設定，然後按一下 [繼續]。

第　39　章

與封存檔案一起運作

封存某些檔案後，您可以使用 Data Backup 與其一起運作。您封存的檔案將以傳統的檔案總管檢視畫面呈現，讓您可以輕易地找到它們。當您的封存增加時，您可能要對這些檔案進行排序或搜尋。您也可於檔案總管檢視畫面中直接開啓檔案，來檢查內容而無需擷取檔案。

若您檔案的本機副本已過時、遺失或損毀，則您可從封存擷取檔案。Data Backup 同時也提供您管理您本機封存與儲存媒體所需的資訊。

在本章中

使用本機封存檔案總管

本機封存檔案總管可讓您檢視並操縱您已在本機封存的檔案。您可檢視每個檔案的名稱、類型、位置、大小、狀態 (已封存、未封存，或封存正在進行中)，及每個檔案最後封存的日期。您亦可按這些條件的任何一項進行排序。

如果您有大的封存，您可以藉由搜尋檔案以快速找到它。您可搜尋完整或部分的檔案名稱或路徑，然後藉由指定最後一次封存時大致的檔案大小與日期來縮小您的搜尋。

找到檔案後，您可於本機封存檔案總管中直接將其開啓。Data Backup 在其自身的程式中開啓檔案，可讓您進行變更而無需離開本機封存檔案總管。該檔案儲存於您電腦上的原始觀察位置，並根據您已定義的封存排程自動進行封存。

排序封存的檔案

您可依下列條件排序您的已封存檔案與資料夾：名稱、檔案類型、大小、狀態 (亦即，已封存、未封存，或封存正在進行中)，檔案最後封存的日期，或您電腦 (路徑) 上的檔案位置。

若要排序封存的檔案：

1 按一下 [本機封存] 索引標籤。

2 在右窗格中，按一下欄位名稱。

搜尋封存的檔案

如果您有大的已封存檔案存放庫，您可以藉由搜尋檔案以快速找到它。您可尋找完整或部分的檔案名稱或路徑，然後藉由指定最後一次封存時大致的檔案大小與日期來縮小您的搜尋。

若要搜尋封存的檔案：

1 在螢幕頂端的 [搜尋] 方塊中鍵入完整或部分的檔案名稱，然後按 ENTER。

2 於 [完整或部分路徑] 方塊中鍵入完整或部分的路徑。

3 執行下列其中一項來指定您正在搜尋之檔案大約的大小：

- 按一下 [< 100 KB]、[< 1 MB]，或 [> 1 MB]。
- 按一下 [大小 (KB)]，然後於方塊中指定大約的大小值。

4 執行下列其中一項來指定檔案最後一次線上備份的日期：

- 按一下 [本週]、[本月] 或 [今年]。

- 按一下 [指定日期]，按一下清單中的 [封存]，然後按一下日期清單中的大約日期值。

5 按一下 [搜尋]。

注意： 若您不知道最後一次封存大致的大小與日期，請按一下 [不明]。

開啟封存檔案

您可直接在本機封存檔案總管中開啟封存的檔案來檢查其內容。

若要開啟封存的檔案：

1 按一下 [本機封存] 索引標籤。

2 在右窗格中，按一下檔案名稱，然後按一下 [開啟]。

秘訣： 您也可以在已封存的檔案名稱上按兩下來開啟該檔。

還原封存的檔案

如果觀察檔案遭到損毀、遺失，或錯誤地刪除，您可從本機封存還原副本。基於這個理由，請確保您定期封存檔案。您亦可還原本機封存檔案較舊的版本。例如，若您定期封存檔案，但想要恢復至檔案的前一個版本，您可於封存位置中找到檔案。如果封存位置是本機磁碟或網路磁碟，則您可以瀏覽檔案。如果封存位置是外接硬碟或 USB 磁碟機，則您必須將磁碟機連接至電腦，然後瀏覽檔案。如果封存位置是 CD 或 DVD，則您必須將 CD 或 DVD 放入電腦，然後瀏覽檔案。

您亦可從不同的電腦還原封存於某部電腦上的檔案。例如，若您在電腦 A 上的外接硬碟對一組檔案進行封存，您可以在電腦 B 上還原這些檔案。要執行此作業，您必須在電腦 B 上安裝 McAfee Data Backup，並連接外接硬碟。然後，於 Data Backup 中，您瀏覽檔案並將其新增至 [遺失的檔案] 清單以進行復原。

如需封存檔案的詳細資訊，請參閱封存檔案。如果您故意要從封存刪除觀察，您亦可從 [遺失的檔案] 清單刪除該項目。

還原本機封存的遺失檔案

Data Backup 的本機封存可讓您復原您電腦上觀察資料夾遺失的資料。例如，若檔案從觀察資料夾移出或遭到刪除，且已經封存，則您可從本機封存還原。

若要還原本機封存的遺失檔案：

1 按一下 [本機封存] 索引標籤。

2 在螢幕底部的 [遺失的檔案] 索引標籤，選取您要還原之檔案名稱旁的核取方塊。

3 按一下[還原]。

秘訣：您可按一下 [全部還原] 來移除 [遺失的檔案] 中所有的檔案。

還原本機封存較舊版本的檔案

如果您還原較舊版本的封存檔案，您可將其找出，並加至 [遺失的檔案] 清單。然後，您可還原該檔案，就如同您對 [遺失的檔案] 清單中的其他檔案一樣。

若要還原本機封存較舊版本的檔案：

1 按一下 [本機封存] 索引標籤。

2 在螢幕底部的 [遺失的檔案] 索引標籤上，按一下 [瀏覽]，然後導覽至儲存封存的位置。

   封存的資料夾名稱具有下列格式：cre ddmmyy_hh-mm-ss_***，其中 ddmmyy 是封存檔案的日期，hh-mm-ss 是封存檔案的時間，而 *** 是 Full 或 Inc 則依據是否執行完整或快速封存而定。

3 選擇位置，然後按一下 [確定]。

   包含於選取位置的檔案出現於 [遺失的檔案] 清單中，可以進行還原。如需更多資訊，請參閱還原本機封存的遺失檔案。

從遺失的檔案清單移除檔案。

當封存檔案從觀察資料夾移出或遭到刪除時，其會自動顯示於 [遺失的檔案] 清單中。這會對封存的檔案與包含於觀察資料夾中的檔案間不一致的狀況發出警示。如果該檔案從觀察的資料夾移出或遭到故意刪除，則您可從 [遺失的檔案] 清單刪除檔案。

若要從遺失的檔案清單移除檔案：

1 按一下 [本機封存] 索引標籤。

2 在螢幕底部的 [遺失的檔案] 索引標籤，選取您要移除之檔案名稱旁的核取方塊。

3 按一下 [刪除]。

秘訣：您可按一下 [全部刪除] 來移除 [遺失的檔案] 中所有的檔案。

管理封存

您可以隨時檢視有關完整與快速封存的資訊摘要。例如，您可檢視目前受到觀察之資料量、已封存的資料量、及目前正在觀察但尚未封存之資料量等的相關資訊。您亦可檢視有關封存排程的資訊，如上次及下次封存發生的日期。

檢視您封存活動的摘要

您可以隨時檢視您封存活動的資訊。例如，您可以檢視已封存的檔案百分比、正在觀察的資料大小、已封存的資料大小，與正在觀察但尚未封存的資料大小。您亦可檢視上次及下次封存發生的日期。

若要檢視您備份活動的摘要：

1 按一下 [本機封存] 索引標籤。

2 在螢幕的頂端，按一下 [帳戶摘要]。

第　40　章

McAfee EasyNetwork

McAfee® EasyNetwork 可以在家用網路的電腦之間進行安全的檔案共用、簡化檔案傳輸，並將印表機共用自動化。

開始使用 EasyNetwork 之前，請先熟悉一些最常用的功能。EasyNetwork 說明中會提供有關設定和使用這些功能的詳細資料。

在本章中

功能

EasyNetwork 提供了下列功能。

檔案共用

EasyNetwork 可使網路上的其他電腦更易共用您電腦上的檔案。共用檔案時，您需要對其他電腦授與這些檔案的唯讀存取權。僅受管理網路的成員電腦 (亦即，具完整或管理存取權) 可共用檔案或存取其他成員所共用的檔案。

檔案傳輸

您可將檔案傳送至受管理網路的其他成員電腦。當您接收檔案時，它會出現在您的 EasyNetwork 收件匣中。收件匣是一個暫時的儲存位置，用來存放網路上其他電腦傳送給您的所有檔案。

自動印表機共用

加入受管理網路後，EasyNetwork 會自動共用任何連至您電腦的本機印表機，並使用印表機現有的名稱作爲共用的印表機名稱。它也會偵測網路上其他電腦所共用的印表機，並讓您設定及使用這些印表機。

第 41 章

設定 EasyNetwork

使用 EasyNetwork 功能之前，您必須先啓動程式，並加入受管理網路。加入網路之後，您可以隨時決定離開網路。

在本章中

啟動 EasyNetwork

依預設，系統在安裝完成後會立刻提示您啟動 EasyNetwork，但是，您也可以稍後再啟動 EasyNetwork。

啟動 EasyNetwork

依預設，系統會提示您在安裝完成後立刻啟動 EasyNetwork，但是，您也可以稍後再啟動 EasyNetwork。

若要啟動 EasyNetwork：

- 在 [開始] 功能表上，依序指向 [程式集]、[McAfee]，然後按一下 [McAfee EasyNetwork]。

秘訣：如果您在安裝期間同意建立桌面圖示和快速啟動圖示，則您也可以按兩下桌面上的 McAfee EasyNetwork 圖示來啟動 EasyNetwork，或按一下工作列右側通知區域中的 McAfee EasyNetwork 圖示來啟動 EasyNetwork。

加入受管理網路

安裝 SecurityCenter 之後，網路代理程式會新增到您的電腦，並在背景中執行。EasyNetwork 中的網路代理程式會負責偵測有效的網路連線、偵測要共用的本機印表機，並監視網路狀態。

如果您目前所連線的網路上找不到正在執行此網路代理程式的其他電腦，則您會自動成爲網路的成員，系統也會提示您識別這是否爲信任的網路。因爲您的電腦是第一部加入網路的電腦，所以網路名稱中會包含您的電腦名稱；但是您可以隨時將網路重新命名。

當電腦連線至網路時，加入請求會傳送至目前網路上的所有其他電腦。網路上任何具有系統管理權限的電腦都可以允許請求。授權者也可以決定目前正加入網路之電腦的權限等級，例如，來賓存取權 (僅具有檔案傳輸的功能) 或完整/系統管理存取權 (具有檔案傳輸和檔案共用的功能)。在 EasyNetwork 中，具有系統管理存取權的電腦可以將存取權授予其他電腦及管理權限 (意即，將電腦升級或降級)，而具有完整存取權的電腦則無法執行這些系統管理工作。允許加入電腦之前，也已經執行過安全檢查。

注意：加入電腦之後，如果您還在電腦上安裝其他 McAfee 網路程式 (例如，McAfee Wireless Network Security 或 Network Manager)，則它也會被當做受那些程式所管理的電腦。指派給電腦的權限等級會套用至所有 McAfee 網路程式。針對來賓權限、完整權限或系統管理權限在其他 McAfee 網路程式中的意義，請參閱該程式所提供的說明文件，以取得詳細資訊。

加入網路

安裝 EasyNetwork 之後，第一次將電腦連線至信任的網路時，系統會出現提示訊息，詢問您是否要加入受管理網路。當電腦同意加入網路時，加入請求會傳送至網路上具有系統管理存取權的所有其他電腦。此請求必須先獲得允許，電腦才能在網路上共用印表機或檔案，或傳送和複製檔案。如果此電腦是網路上第一部電腦，則它會自動獲得網路上的系統管理權限。

若要加入網路：

1. 在 [共用檔案] 視窗中，按一下 [是，現在就加入網路]。
   當網路上的系統管理電腦允許您的請求時會出現訊息，詢問是否要允許此電腦和網路上的其他電腦管理彼此的安全性設定。
2. 若要允許此電腦和網路上的其他電腦管理彼此的安全性設定，請按一下 [是]，否則，請按一下 [否]。
3. 確認允許的電腦所顯示的圖片是否與目前安全性確認對話方塊中顯示的圖片相同，然後按一下 [確認]。

注意：如果允許的電腦所顯示的圖片與安全性確認對話方塊中顯示的圖片不同，則表示受管理網路上發生安全漏洞。加入網路可能會讓您的電腦面臨風險，因此，請按一下安全性確認對話方塊中的 [拒絕]。

授予對網路的存取權

當電腦請求加入受管理網路時，訊息會傳送至網路上具有系統管理存取權的所有其他電腦。第一部對訊息做出回應的電腦會成爲授權者。如果您是授權者，則您必須負責決定要授予此電腦的存取權類型：來賓存取權、完整存取權或系統管理存取權。

若要授予對網路的存取權：

1. 在警示中，選取下列其中一個核取方塊：
   - 授予來賓存取權：允許使用者將檔案傳送至其他電腦，但使用者無法共用檔案。
   - 授予對所有受管理網路應用程式的完整存取權：允許使用者傳送和共用檔案。
   - 授予對所有受管理網路應用程式的系統管理存取權：允許使用者傳送和共用檔案、將存取權授予其他電腦，並調整其他電腦的權限等級。

2 按一下 [授予存取權]。

3 確認電腦所顯示的圖片是否與目前安全性確認對話方塊中顯示的圖片相同，然後按一下 [確認]。

注意：如果電腦所顯示的圖片與安全性確認對話方塊中顯示的圖片不同，則表示受管理網路上發生安全漏洞。將網路存取權授予此電腦可能會讓您的電腦面臨風險，因此，請按一下安全性確認對話方塊中的 [拒絕]。

重新命名網路

依預設，網路名稱包含第一部加入網路之電腦的名稱；但是您可以隨時變更網路名稱。當您重新命名網路時，您可以變更 EasyNetwork 中顯示的網路說明。

若要重新命名網路：

1. 在 [選項] 功能表上，按一下 [設定]。
2. 在 [設定] 對話方塊的 [網路名稱] 方塊中，輸入網路名稱。
3. 按一下 [確定]。

離開受管理網路

如果您在加入受管理網路之後，決定不想繼續成為網路成員，您可以離開網路。放棄成員資格後，可以隨時重新加入，但是您必須重新取得加入和執行安全性檢查的權限。如需詳細資訊，請參閱加入受管理網路 (第 255 頁)。

離開受管理網路

您可以離開先前加入的受管理網路。

若要離開受管理網路：

1 在 [工具] 功能表上，按一下 [離開網路]。
2 在 [離開網路] 對話方塊中，選取您想要離開的網路名稱。
3 按一下 [離開網路]。

第 42 章

共用和傳送檔案

EasyNetwork 讓您的電腦可以輕鬆地與網路上的其他電腦共用和傳送檔案。共用檔案時，您需要對其他電腦授與這些檔案的唯讀存取權。僅受管理網路成員的電腦 (亦即，具完整或管理存取權) 可共用檔案或存取其他成員電腦所共用的檔案。

在本章中

共用檔案

EasyNetwork 可使網路上的其他電腦更易共用您電腦上的檔案。共用檔案時，您需要對其他電腦授與這些檔案的唯讀存取權。僅受管理網路成員的電腦 (亦即，具完整或管理存取權) 可共用檔案或存取其他成員電腦所共用的檔案。如果您共用資料夾，則該資料夾及子資料夾中的所有檔案都會共用，但是之後新增至資料夾的檔案則不會自動共用。如果刪除共用的檔案或資料夾，則 [共用檔案] 視窗中會自動移除這些檔案或資料夾。您可以隨時停止共用檔案。

存取共用的檔案有兩種方法：直接從 EasyNetwork 開啟檔案，或將檔案複製到您的電腦上再加以開啟。如果共用檔案的清單變得很長，您可以搜尋想要存取的共用檔案。

注意：使用 EasyNetwork 共用的檔案無法從使用 Windows 檔案總管的其他電腦進行存取。EasyNetwork 檔案共用會透過安全連線來執行。

共用檔案

當您共用檔案時，對受管理網路具有完整存取權或系統管理存取權的所有其他成員都自動可以使用這個檔案。

若要共用檔案：

1. 在 Windows 檔案總管中，尋找您想要共用的檔案。
2. 將檔案從 Windows 檔案總管中拖曳到 EasyNetwork 的 [共用的檔案] 視窗。

秘訣：您也可以按一下 [工具] 功能表上的 [共用檔案] 來共用檔案。在 [共用] 對話方塊中，導覽至您想要共用的檔案所存放的資料夾、選取檔案，然後按一下 [共用]。

停止共用檔案

如果您在受管理網路上共用檔案，則可以隨時停止共用檔案。當您停止共用檔案時，受管理網路上的其他成員就再也無法存取此檔案了。

若要停止共用檔案：

1. 在 [工具] 功能表上，按一下 [停止共用檔案]。
2. 在 [停止共用檔案] 對話方塊中，選取您不想再繼續共用的檔案。
3. 按一下 [不共用]。

複製共用的檔案

您可以將共用的檔案，從受管理網路上的任何電腦複製到您的電腦。如果電腦之後停止共用檔案，您仍舊保有副本。

若要複製檔案：

- 將檔案從 EasyNetwork 的 [共用檔案] 視窗拖曳到 Windows 檔案總管或 Windows 桌面上。

> **秘訣：**您也可以選取 EasyNetwork 中的檔案，然後按一下 [工具] 功能表上的 [複製到]，來複製共用的檔案。在 [複製到資料夾] 對話方塊中，導覽至您想要複製檔案的資料夾、選取資料夾，然後按一下 [儲存]。

搜尋共用的檔案

您可以搜尋由您或任何其他網路成員所共用的檔案。當您輸入搜尋條件時，EasyNetwork 會自動在 [共用的檔案] 視窗顯示對應的結果。

若要搜尋共用的檔案：

1. 在 [共用的檔案] 視窗中，按一下 [搜尋]。
2. 按一下 [包含] 清單中的下列其中一個選項：
   - **包含所有文字**：在 [檔案或路徑名稱] 清單中，搜尋包含您所指定的所有文字之檔案名稱或路徑名稱 (不依順序排列)。
   - **包含任何文字**：在 [檔案或路徑名稱] 清單中，搜尋包含您所指定的任何文字之檔案名稱或路徑名稱。
   - **包含完全符合的字串**：在 [檔案或路徑名稱] 清單中，搜尋包含與您所指定的字串完全符合之檔案名稱或路徑名稱。
3. 在 [檔案或路徑名稱] 清單中輸入部分或完整的檔案名稱或路徑。
4. 按一下 [類型] 清單中的下列其中一個檔案類型：
   - **任何**：搜尋所有共用的檔案類型。
   - **文件**：搜尋所有共用的文件。
   - **影像**：搜尋所有共用的影像檔案。
   - **視訊**：搜尋所有共用的視訊檔案。
   - **音訊**：搜尋所有共用的音訊檔案。
5. 在 [開始時間] 與 [結束時間] 清單中，按一下代表檔案建立日期範圍的日期。

將檔案傳送至其他電腦

您可將檔案傳送至受管理網路的其他成員電腦。傳送檔案之前，EasyNetwork 會先確認接收檔案的電腦是否有足夠的可用硬碟空間。

當您接收檔案時，它會出現在您的 EasyNetwork 收件匣中。收件匣是一個暫時的儲存位置，用來存放網路上其他電腦傳送給您的所有檔案。如果您在接收檔案時開啟 EasyNetwork，則檔案會立即出現在您的收件匣中，否則，在 Windows 工作列右側的通知區域中會出現訊息。如果您不想收到通知訊息，可以關閉此功能。如果收件匣中已經有同名的檔案，則新的檔案會加上數值尾碼來重新命名。在您接受檔案 (意即，將檔案複製到您的電腦) 之前，檔案會留在您的收件匣中。

將檔案傳送到另一部電腦

您可以直接將檔案傳送到受管理網路上的另一部電腦，而不需再共用檔案。接收者電腦上的使用者必須先將檔案儲存至本機位置，才能檢視檔案。如需詳細資訊，請參閱從另一部電腦接受檔案 (第 264 頁)。

若要將檔案傳送到另一部電腦：

1 在 Windows 檔案總管中，尋找您想要傳送的檔案。

2 將檔案從 Windows 檔案總管中拖曳到 EasyNetwork 的作用中電腦圖示。

秘訣：在選取檔案時按住 CTRL 鍵，就可以將多個檔案傳送至電腦。您也可以按一下 [工具] 功能表上的 [傳送]、選取檔案，然後按一下 [傳送]，來傳送檔案。

從另一部電腦接受檔案

如果受管理網路上的另一部電腦傳送檔案給您，您必須接受它 (將檔案儲存到您電腦上的資料夾)。當檔案傳送至您的電腦時，如果您未開啟 EasyNetwork，或 EasyNetwork 不在幕前，則您會在工作列右側的通知區域中收到通知訊息。按一下通知訊息，即可開啟 EasyNetwork 並存取檔案。

若要接收另一部電腦的檔案：

- 按一下 [接受]，然後將檔案從 EasyNetwork 收件匣拖曳至 Windows 檔案總管中的資料夾。

秘訣：您也可以選取 EasyNetwork 收件匣中的檔案，再按一下 [工具] 功能表上的 [接受]，接收另一部電腦的檔案。在 [接受到資料夾] 對話方塊中，導覽至您想要儲存所接收的檔案之資料夾、選取資料夾，然後按一下 [儲存]。

在檔案傳送時收到通知

當受管理網路上的另一部電腦傳送檔案給您時，您可以收到通知。如果目前未開啓 EasyNetwork，或 EasyNetwork 不在幕前的桌面上，則 Windows 工作列右側的通知區中會出現通知訊息。

若要在檔案傳送時收到通知：

1. 在 [選項] 功能表上，按一下 [設定]。
2. 在 [設定] 對話方塊中，選取 [當其他電腦傳送檔案給我時，請通知我] 核取方塊。
3. 按一下 [確定]。

第 43 章

共用印表機

您加入受管理的網路之後，EasyNetwork 會自動共用連至您電腦的任何本機印表機。它也會偵測網路上其他電腦所共用的印表機，並讓您設定及使用這些印表機。

在本章中

使用共用的印表機

加入受管理網路後，EasyNetwork 會自動共用任何連至您電腦的本機印表機，並使用印表機現有的名稱作爲共用的印表機名稱。它也會偵測網路上其他電腦所共用的印表機，並讓您設定及使用這些印表機。如果您將印表機驅動程式設定爲透過網路列印伺服器 (例如，無線 USB 列印伺服器) 進行列印，EasyNetwork 會將印表機當做本機印表機，並自動在網路上共用此印表機。您也可以隨時停止共用印表機。

EasyNetwork 也會偵測網路上所有其他電腦所共用的印表機。如果它偵測到遠端印表機尚未連線至您的電腦，則當您第一次開啓 EasyNetwork 時，[可用的網路印表機] 連結會出現在 [共用檔案] 視窗中。這可以讓您安裝可用的印表機或解除安裝已經連線至您的電腦的印表機。您也可以重新整理網路上偵測到的印表機之清單。

如果您尚未加入受管理的網路，但卻已經連線至此網路，您可以從標準的 Windows 印表機控制台存取共用的印表機。

停止共用印表機

您可以隨時停止共用印表機。已安裝印表機的成員將無法再透過它進行列印。

若要停止共用印表機：

1 在 [工具] 功能表上，按一下 [印表機]。
2 在 [管理網路印表機] 對話方塊中，按一下您不想繼續共用的印表機名稱。
3 按一下 [不共用]。

安裝可用的網路印表機

只要您是受管理網路的成員，就可以存取網路上共用的印表機。要這樣做，您必須先安裝印表機使用的印表機驅動程式。如果在您安裝印表機之後，它的擁有者停止共用，則您將無法繼續透過該印表機進行列印。

若要安裝可用的網路印表機：

1 在 [工具] 功能表上，按一下 [印表機]。
2 在 [可用的網路印表機] 對話方塊中，按一下印表機名稱。
3 按一下 [安裝]。

第　44　章

參考

「術語字彙」列出並定義 McAfee 產品中最常用的安全性術語。

「關於 McAfee」提供有關 McAfee Corporation 的法律資訊。

字彙

8

802.11

一組無線區域網路技術的 IEEE 標準。802.11 會指定無線用戶端與基地站台之間，或是無線用戶端之間的空中傳輸介面。802.11 的其中多項規格包括：802.11a (用於 5Ghz 頻寬中，傳輸率最高達 54 Mbps 的網路標準)、802.11b (用於 2.4 Ghz 頻寬中，傳輸率最高達 11 Mbps 的網路標準)、802.11g (用於 2.4 Ghz 頻寬中，傳輸率最高達 54 Mbps 的網路標準) 及 802.11i (一套適用於所有無線乙太網路的安全標準)。

802.11a

802.11 的延伸模組，適用於無線區域網路，可在 5GHz 頻寬中，以最高 54 Mbps 的網路傳輸率來傳送資料。雖然傳輸速度比 802.11b 快，但是所覆蓋的距離小很多。

802.11b

802.11 的延伸模組，適用於無線區域網路，可在 2.4 GHz 頻寬中，提供 11 Mbps 的傳輸率。802.11b 目前被視爲無線標準。

802.11g

802.11 的延伸模組，適用於無線區域網路，在 2.4 GHz 頻寬中，最高可提供 54 Mbps 的傳輸率。

802.1x

不受 Wireless Home Network Security 支援。用於有線及無線網路上的 IEEE 驗證標準，但其最知名的用法是與 802.11 無線網路搭配使用。這項標準在用戶端與驗證伺服器之間提供穩健的相互驗證功能。此外，802.1x 可依每位使用者及每個工作階段，提供動態的 WEP 金鑰，免除了管理的負擔，避免靜態 WEP 金鑰周遭的安全風險。

C

cookie

在全球資訊網上，Web 伺服器儲存於用戶端系統上的資料區塊。當使用者回到相同網站時，瀏覽器會將 Cookie 的副本傳回伺服器。Cookie 可用來識別使用者、導引伺服器傳送所要求網頁的自訂版本、提交使用者的帳戶資訊，以及作爲其他管理之用。

Cookie 能讓網站記住您的身份，並追蹤造訪過網站的人數、造訪的時間，以及檢視過的網頁。Cookie 也可以幫助公司爲您個人化它的網站。許多網站會要求使用者名稱及密碼來存取某些網頁，並且會傳送 Cookie 至您的電腦，如此您就不需要每次進行登入手續。然而，Cookie 可以用於惡意的行爲。線上廣告公司經常利用 Cookie 得知您經常造訪的網站，以便在您最喜愛的網站上張貼廣告。在允許網站的 Cookie 之前，請確定您信任該網站。

如果 Cookie 是合法公司的資訊來源，那麼它們也可以是駭客的資訊來源。許多有線上商店的網站，都會將信用卡及其他的個人資訊放在 Cookie 中，以方便客戶購買。可惜，有一些安全上的漏洞會讓駭客從儲存在客戶電腦上的 Cookie 存取資訊。

D

DNS

網域名稱系統 (Domain Name System) 的首字母縮寫。在網際網路上使用的一種分階層的系統，同時具有網域名稱位址 (例如：bluestem.prairienet.org) 及 IP 位址 (例如：192.17.3.4)。網域名稱位址爲一般使用者所使用，並且會自動轉譯成封包遞送軟體所使用的數字 IP 位址。DNS 名稱的組成份子有第一層網域 (例如 .com、.org 及 .net)、第二層網域 (企業、組織或個人的網站名稱)，也可能有一個或多個次網域 (第二層網域中的伺服器)。另請參閱 DNS 伺服器及 IP 位址。

DNS 伺服器

網域名稱系統 (Domain Name System) 伺服器的簡稱。可回應網域名稱系統 (DNS) 查詢的電腦。DNS 伺服器會保留主機電腦及其對應之 IP 位址的資料庫。例如，以 apex.com 名稱顯示時，DNS 伺服器就會傳回假設公司 Apex 的 IP 位址。亦稱爲：名稱伺服器。另請參閱 DNS 及 IP 位址。

E

ESS (延伸服務集)

兩個以上網路的集合，構成單一子網路。

I

IP address (IP 位址)

網際網路通訊協定位址，即 IP 位址，是一組唯一的號碼，包含四段數字，以圓點分隔 (例如 63.227.89.66)。網際網路上每一部電腦，從最大型的伺服器到經由行動電話通訊的膝上型電腦，都有其專用的 IP 號碼。不是每一部電腦都有網域名稱，但是一定都有一個 IP。

以下列出一些罕見的 IP 位址類型：

- 非路由式的 IP 位址：這些位址也稱爲私人 IP 空間。這些是無法在網際網路上使用的 IP 位址。私人 IP 區段爲 10.x.x.x、172.16.x.x - 172.31.x.x 和 192.168.x.x。
- 迴圈 IP 位址：迴圈位址是用於測試的。傳送至 IP 位址的這個區段的流量會再送回產生封包的裝置。它永遠不會與裝置分離，主要是用於硬體及軟體測試。迴圈 IP 區段爲 127.x.x.x。

Null IP 位址：這是無效的位址。如果看見這種位址，表示流量有空白的 IP 位址。這很明顯是不正常的，而且常常代表傳送者故意掩蔽流量的來源。傳送者將無法接收對其流量的任何回應，除非封包被可以理解其內容的應用程式接收到，而封包中會包含只用於該應用程式的指示。所有以 0 開頭的位址 (0.x.x.x) 都是 Null 位址。例如，0.0.0.0 就是 Null IP 位址。

L

LAN (區域網路)

跨越較小區域的電腦網路。大部分的區域網路受限於一棟建築物或一群建築物中。然而，透過電話或無線電波，便能讓一個區域網路與其他任何距離以外的區域網路產生連線。用這種方式連接的區域網路系統，即稱爲廣域網路 (WAN)。大部分的區域網路，一般會透過簡單的集線器或交換器，連接工作站及個人電腦。區域網路中的每個節點 (每一台電腦) 都有自己的 CPU 能執行程式，也能存取任何區域網路上的資料及裝置 (例如：印表機)。這表示許多使用者可以共用昂貴的裝置 (例如：雷射印表機) 以及資料。使用者也可以使用區域網路來互相通訊，例如，藉由傳送電子郵件或加入交談階段。

M

MAC (「媒體存取控制」或「訊息驗證器代碼」)

如需前者資訊，請參閱＜MAC 位址＞。後者是用來識別給定訊息 (例如：RADIUS 訊息) 的代碼。代碼通常是訊息內容的加密強化雜湊碼，其中包含唯一值，可確保重新執行的防護機制。

MAC 位址 (媒體存取控制位址)

指定給存取網路之實體裝置的低階位址。

MAPI 帳戶

訊息應用程式設計介面 (Messaging Application Programming Interface) 的首字母縮寫。Microsoft 的介面規格，能讓不同的訊息及工作群組應用程式 (包括電子郵件、語音訊息及傳真) 可以透過單一用戶端來工作，例如 Exchange 用戶端。基於這個理由，MAPI 通常會用於 Microsoft® Exchange Server 的公司環境中。但是很多人都用 Microsoft 的 Outlook 來處理個人的網際網路電子郵件。

MSN 帳戶

Microsoft 網路 (Microsoft Network) 的首字母縮寫。線上服務及網際網路入口網站。這是以 Web 為基礎的帳戶。

N

NIC (網路介面卡)

插在筆記型電腦或其他裝置上的卡片，可將裝置連接至區域網路。

P

PCI 無線介面卡

將桌上型電腦連線至網路。該卡插在電腦的 PCI 擴充插槽中。

POP3 帳戶

郵局通訊協定 3 (Post Office Protocol 3) 的首字母縮寫。大部分的家庭使用者都有這種類型的帳戶。這是 TCP/IP 網路上普遍使用之「郵局通訊協定」標準的目前版本。亦即所謂的標準電子郵件帳戶。

PPPoE

使用於乙太網路的點對點通訊協定 (Point-to-Point Protocol Over Ethernet)。PPPoE 為眾多 DSL 提供者所使用，可支援 PPP 中廣泛使用的通訊協定層及驗證，並可在乙太網路的標準多點架構中，建立點對點連線。

proxy

構成網路與網際網路間的障礙之電腦 (或是這部電腦上執行的軟體)，它對外部網站僅會顯示一個網路位址。Proxy 的功能就像是代表所有內部電腦的媒介，它可以在保護網路身份的同時，也繼續提供網際網路存取權。另請參閱 Proxy 伺服器。

Proxy 伺服器

一種防火牆元件，負責管理網際網路進出區域網路 (LAN) 的流量。Proxy 伺服器可以提供常用資料 (例如受歡迎的網頁) 以提高效能，還可以篩選、捨棄擁有者認為是不適當的要求 (例如要求專用檔案的未授權存取權)。

R

RADIUS (遠端存取撥入使用者服務)

提供使用者驗證的通訊協定，通常會在遠端存取的內容中。此通訊協定原本定義要搭配撥入遠端存取伺服器使用，現在則用於各種驗證環境中，包括 WLAN 使用者共用密碼的 802.1x 驗證。

S

SMTP 伺服器

簡易郵件傳輸通訊協定 (Simple Mail Transfer Protocol) 的首字母縮寫。將訊息從一部電腦傳送至網路上另一部電腦時，所使用的 TCP/IP 通訊協定。此通訊協定可用在網際網路上遞送電子郵件。

SSID (服務組識別碼)

無線區域網路子系統中之裝置的網路名稱。這是新增至每個 WLAN 封包標題，32 字元字串的純文字。SSID 會區分 WLAN，因此網路的所有使用者都必須提供相同的 SSID，才能存取某個給定的 AP。SSID 會防止任何沒有 SSID 的用戶端裝置進行存取。但是依預設，存取點 (AP) 會在其指標中廣播其 SSID。即使關閉 SSID 廣播功能，駭客仍可透過探查來偵測 SSID。

SSL (安全通訊端層)

Netscape 開發的通訊協定，可透過網際網路來傳輸私人文件。SSL 使用公開金鑰來工作，加密透過 SSL 連線傳送的資料。Netscape Navigator 及 Internet Explorer 都能使用並支援 SSL，而且許多網站都使用通訊協定來取得機密使用者資訊，例如信用卡號碼。依照慣例，需要 SSL 連線的 URL 都會以 https: 開頭，而不是 http:。

SystemGuard

SystemGuard 會偵測電腦上未經授權的變更，並在發生變更時警示您。

T

TKIP (暫時金鑰完整性協定)

能克服 WEP 安全性中固有弱點的快速解決方法，尤其是重複使用加密金鑰的問題。每 10,000 個封包，TKIP 會變更一次暫時金鑰，提供動態散發方法，可大幅加強網路的安全性。TKIP (安全性) 程序是從用戶端與存取點 (AP) 之間共用的 128 位元暫時金鑰開始。TKIP 合併暫時金鑰與 (用戶端機器的) MAC 位址，然後加入相對較大的 16 個八位元初始化向量，以產生用來加密資料的金鑰。這個程序可確保每個站台用來加密資料的金鑰資料流都不一樣。TKIP 會使用 RC4 來執行加密作業。WEP 也會使用 RC4。

U

URL

統一資源定位器。此爲網際網路位址的標準格式。

USB 無線介面卡

提供可擴充的隨插即用序列介面。這個介面可爲周邊裝置 (例如：鍵盤、滑鼠、搖桿、印表機、掃描器、儲存裝置及視訊會議相機) 提供標準、低成本的無線連線。

V

VPN (虛擬私人網路)

使用公眾線路來重新聚集節點，進而建構的網路。例如，有很多系統都可以讓您使用網際網路來作爲傳輸資料的媒介，以建立網路。這些系統會使用加密及其他安全機制，以確保唯有經授權的使用者才能存取網路，而且無法攔截該資料。

W

WEP (有線等效隱私)

定義爲 802.11 標準一部分的加密及驗證通訊協定。初始版本以 RC4 密碼爲基礎，並具有重大的弱點。WEP 會嘗試透過無線電波來加密資料，以提供安全性，讓資料可以在端點之間傳送時獲得保護。但是，我們發現 WEP 並沒有我們想像中的安全。

Wi-Fi (無線相容認證)

指任何類型的 802.11 網路時 (無論是 802.11b、802.11a、雙頻等等)，通常都會用到。該術語爲 Wi-Fi 聯盟 (Wi-Fi Alliance) 所使用。

Wi-Fi 認證

經由 Wi-Fi 聯盟測試並核准爲 Wi-Fi Certified (註冊商標) 的任何產品，都是經過認證，可彼此互相操作，即使是來自不同製造商的產品也是一樣。擁有 Wi-Fi Certified 產品的使用者，可將任何品牌的存取點 (AP) 用於亦經認證的任何其他品牌用戶端硬體。但是通常使用相同無線電頻率的任何 Wi-Fi 產品 (例如：用於 802.11b 或 11g 的 2.4GHz、用於 802.11a 的 5GHz)，即使沒有 Wi-Fi Certified，仍可一起運作。

Wi-Fi 聯盟 (Wi-Fi Alliance)

由無線設備及軟體的領導提供者所組成的組織，其使命爲：(1) 認證所有 802.11 產品的互相操作能力，以及 (2) 任何 802.11 無線區域網路產品的所有市場，將 Wi-Fi 這個術語推廣爲全球性的品牌名稱。該組織的性質就像協會、測試實驗室，以及想要提升互相操作能力及產業成長之廠商的情報交流站。

雖然所有 802.11a/b/g 產品皆稱爲 Wi-Fi，但是只有通過 Wi-Fi 聯盟測試的產品，才能聲稱其產品爲 Wi-Fi Certified (註冊商標)。通過的產品必須在其包裝上附加認證標章 (Wi-Fi Certified)，並指出所使用的無線電頻道。這個集團原名爲無線乙太相容性聯盟 (WECA)，但在 2002 年 10 月更名，以期更能反映其所要建立的 Wi-Fi 品牌。

WLAN (無線區域網路)

請參閱＜LAN＞。使用無線媒介來連線的區域網路。WLAN 會使用高頻無線電波 (而非有線)，在節點之間通訊。

WPA (受 Wi-Fi 保護的存取)

可針對現有及未來無線區域網路系統，強力提升資料保護和存取控制層級的規格標準。WPA 的設計可在現有的硬體上執行，作爲軟體升級，WPA 衍生自 IEEE 802.11i 標準，並與其相容。若安裝得當，可爲無線區域網路使用者高度保證其資料會持續受到保護，而且只有經授權的網路使用者才能存取網路。

WPA-PSK

專爲家庭使用者設計的特殊 WPA 模式，家庭使用者不需要強大的企業級安全性，也沒有驗證伺服器的存取權。在此模式下，家庭使用者要手動輸入啓動密碼，以「預先共用金鑰」模式來啓動「受 Wi-Fi 保護的存取」，並且要經常變更每部無線電腦及存取點的密碼。另請參閱＜WPA2-PSK 及 TKIP＞。

WPA2

另請參閱＜WPA＞。WPA2 是 WPA 安全標準的更新，以 802.11i IEEE 標準爲基礎。

WPA2-PSK

另請參閱＜WPA-PSK 及 WPA2＞。WPA2-PSK 類似 WPA-PSK，以 WPA2 標準爲基礎。WPA2-PSK 其中一項常見的功能，就是裝置通常會同時支援多種加密模式 (例如：AES、TKIP)，而較舊的裝置通常一次只能支援一種加密模式 (亦即，所有用戶端都必須使用相同的加密模式)。

一劃

一般文字

任何未加密的訊息。

四劃

內容分級群組

使用者所屬的年齡組。依據使用者所屬的內容分級群組來分級 (亦即可用或封鎖) 內容。內容分級群組包括：幼兒、幼童、青少年、少年及成人。

五劃

加密

一種程序，將文字資料轉換成密碼，使資訊變得混亂難懂，讓不知道如何解密的人無法閱讀。

外接式硬碟

裝在電腦機箱外的硬碟機。

未成年保護

可以讓您設定內容分級和網際網路時間限制的設定，前者會限制使用者可以檢視的網站和內容，後者則指定使用者可以存取網際網路的期間和持續時間。未成年保護還可讓您全面限制對特定網站的存取權，並依據年齡群組及關聯的關鍵字，授權或封鎖存取權。

用戶端

在個人電腦或工作站上執行，並仰賴伺服器來執行某些作業的應用程式。例如，電子郵件用戶端是可以讓您傳送及接收電子郵件的應用程式。

白名單

容許存取的網站清單，因為這些網站被認為不具詐騙性。

六劃

企業內部網路

私人網路，通常位於機構或企業的內部，功能與網際網路十分類似。這種方式可讓學生或員工使用校外或遠距的獨立作業電腦來存取內部網路，已經變得十分普遍。防火牆、登入程序及密碼都是為了提供安全而設計的。

共用

一項作業，可以讓電子郵件收件者在一段有限時間內存取選取的備份檔案。您共用檔案時，會將檔案的備份副本傳送至您指定的電子郵件收件者。收件者會收到 Data Backup 寄送的電子郵件，指出已和收件者共用檔案。電子郵件也會包含到共用檔案的連結。

共用密碼

另請參閱＜RADIUS＞。保護 RADIUS 訊息的機密部分。此共用密碼是驗證器與驗證伺服器之間，以某種安全方式來共用的密碼。

同步

解決備份檔案與您本機電腦上儲存之檔案不一致的情形。線上備份存放庫中的檔案版本比其他電腦上的檔案版本還要新時，您要將檔案同步。同步會利用線上備份存放庫中的檔案版本，更新您電腦上的檔案副本。

字典攻擊

這種攻擊會嘗試使用清單中的大量文字來判斷使用者的密碼。攻擊者不會手動嘗試所有組合，而是會利用工具來自動試探，以找出使用者的密碼。

存取點 (AP)

一種能讓 802.11 用戶端連接到區域網路 (LAN) 的網路裝置。AP 可為無線使用者擴充服務的實體範圍。有時亦稱為無線路由器。

七劃

伺服器

一部電腦或一套軟體，為其他電腦上執行之軟體提供特定的服務。您的 ISP 的「郵件伺服器」是處理它的所有使用者的所有內送及外寄郵件的軟體。區域網路上的伺服器是組成網路上主要節點的硬體。伺服器也可能配備軟體，為所有相連的用戶端電腦提供特定服務、資料或其他功能。

即時掃描

當您或您的電腦存取檔案時，會掃描該檔案是否有病毒或其他活動。

完整封存

根據您設定的觀察檔案類型與位置，封存完整的資料集。

快速封存

只封存自上次完整或快速封存之後，變更過的觀察檔。

快顯視窗

一些小視窗，會在您電腦螢幕上其他視窗之上顯示。快顯視窗通常是在 Web 瀏覽器中，用來顯示廣告。McAfee 會封鎖在您的瀏覽器載入網頁時自動載入的快顯視窗。但是不會封鎖您按下連結時載入的快顯視窗。

防火牆

一套專門用來防止在未經授權的情況下，與私人網路往來存取的系統。防火牆可部署於硬體及軟體，或是軟硬體的組合中。人們經常使用防火牆來防止未經授權的網際網路使用者，存取連線至網際網路的私人網路，尤其是內部網路。所有進出內部網路的訊息都要經過防火牆。防火牆會檢查每則訊息，並封鎖不符指定安全條件的訊息。防火牆被視為保護私人資訊的第一道防線。若要加強安全性，可將資料加密。

八劃

事件

來自 0.0.0.0 的事件

如果您看到來自 IP 位址 0.0.0.0 的事件，可能的原因有兩種。 第一種，也是最常見的，就是您的電腦因故收到了格式錯誤的封包。 網際網路並不是可以永遠完全信賴的，有時也會有錯誤的封包。由於防火牆會在 TCP/IP 驗證之前看到封包，因此可能會將這些封包報告爲事件。

另一種情況就是來源 IP 是僞造的。 僞造的封包表示可能有人正在到處尋找特洛伊病毒，而且他們剛好就是在試您的電腦。請記住防火牆會封鎖嘗試，這是很重要的。

來自 127.0.0.1 的事件

事件有時會列出它們的來源 IP 爲 127.0.0.1。請特別注意這是特殊的 IP，稱爲迴圈位址。

無論您正在使用哪一部電腦，127.0.0.1 指的一律爲您的本機電腦。此類位址亦稱爲 Localhost，因爲電腦名稱 localhost 一定會解析回 IP 位址 127.0.0.1。這表示您的電腦正嘗試入侵它自己嗎？特洛伊病毒或間諜軟體正在掌控您的電腦嗎？不可能。許多合法的程式都是使用迴圈位址來進行元件之間的通訊。例如，許多個人郵件或 Web 伺服器都會讓您透過 Web 介面來進行設定，而該介面通常都可以透過像是 http://localhost/ 這一類的網址來存取。

然而，防火牆允許來自這些程式的資料流，因此如果您看到來自 127.0.0.1 的事件，很可能是表示來源 IP 位址是僞造的。僞造的封包通常表示有人正在到處尋找特洛伊病毒。請記住防火牆會封鎖這類嘗試，這是很重要的。顯而易見地，報告來自 127.0.0.1 的事件並沒有幫助，所以不需要這麼做。

因此，有一些程式，特別是 Netscape 6.2 及更新的版本，會要求您將 127.0.0.1 新增到 [信任的 IP 位址] 清單中。這些程式的元件之間進行通訊的方式，使得防火牆無法判斷流量是否來自本機。

在 Netscape 6.2 中，如果您不信任 127.0.0.1，就無法使用您的信任的 IP 清單。因此，如果您看到來自 127.0.0.1 的流量，而且您電腦上所有的程式都正常運作，那麼封鎖此流量就是安全的。但是，如果程式 (如 Netscape) 有問題，請在防火牆中的 [信任的 IP 位址] 清單中新增 127.0.0.1，看看是否能解決問題。

如果將 127.0.0.1 放在 [信任的 IP 位址] 清單中可以解決問題，那麼您必須衡量選擇：如果您信任 127.0.0.1，您的程式就可以運作，但是您對於僞造攻擊就更沒有防範了。如果您不信任該位址，您的程式將無法運作，但是您仍舊可以受到保護，不被此類具攻擊性的流量所攻擊。

來自您區域網路上電腦的事件

就大部分公司的區域網路設定而言，您可以信任區域網路上的所有電腦。

來自私人 IP 位址的事件

192.168.xxx.xxx、10.xxx.xxx.xxx 和 172.16.0.0 - 172.31.255.255 格式的 IP 位址稱爲非路由式的位址或私人 IP 位址。這些 IP 位址應該永遠不與您的網路分離，而且大多數時候都可以信任。

192.168 區段是搭配 Microsoft「網際網路連線共用」(ICS) 使用的。如果您使用 ICS，而且看到來自此 IP 區段的事件，您可以將 IP 位址 192.168.255.255 新增到 [信任的 IP 位址] 清單中。 如此將會信任整個 192.168.xxx.xxx 區段。

如果您不是在私人網路上，但卻看到來自這些 IP 範圍的事件，則來源 IP 位址可能就是偽造的。偽造的封包通常代表有人正在到處尋找特洛伊病毒。請記住防火牆會封鎖這類嘗試，這是很重要的。

因為私人 IP 位址與網際網路中的 IP 位址是分開的，所以報告這些事件不會有任何作用。

受管理網路

包含兩種成員的家庭網路：受管理成員與不受管理成員。受管理成員可讓網路上其他電腦監視其 McAfee 保護狀態；而不受管理成員則否。

拒絕服務

在網際網路上的「拒絕服務 (DoS)」攻擊事件中，使用者或組織正常情形下應該享有的資源服務會被剝奪。一般而言，喪失服務就是特定的網路服務無法正常運作 (例如電子郵件)，或是暫時失去所有的網路連線及服務。例如，最糟的情況有時候是，供數百萬人存取的網站可能被迫暫停運作。拒絕服務攻擊也可能會損毀電腦系統中的程式設計及檔案。雖然拒絕服務通常是蓄意製造成並帶有惡意，但是有時也可能在非刻意的情況下，發生拒絕服務攻擊。拒絕服務攻擊為一種電腦系統的安全缺口，通常不會造成資訊遭竊取或其他安全上的損失。然而，這些攻擊會耗費目標使用者或公司大量的時間與金錢。

金鑰

由二個裝置用來驗證其通訊作業的一串字母及/或數字。這二個裝置都必須要有這個金鑰。另請參閱 WEP、WPA、WPA2、WPA-PSK 及 WPA2- PSK。

九劃

封存

在本機的 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟機上，建立觀察檔的副本。

封存

在本機的 CD、DVD、USB 磁碟機、外接硬碟或網路磁碟機上，建立觀察檔的副本。

指令碼

指令碼可以建立、複製或刪除檔案。亦可開啓您的 Windows 登錄。

十劃

特洛伊病毒

特洛伊程式會假裝成無惡意應用程式。特洛伊程式不是病毒，因為它不會複製，但其攻擊性可以跟病毒一樣強。

十一劃

偽造 IP

在 IP 封包中偽造 IP 位址。在很多類型的攻擊中，都會使用這種手法，包括工作階段挾持。人們也經常使用此方法，偽造垃圾電子郵件的標題，讓他人難以正確追蹤。

密碼

一組代碼 (通常是英數字元)，您使用這組代碼取得您電腦、指定之程式或網站的存取權。

密碼文字

加密的資料。密碼文字必須使用金鑰來 (解密) 轉換成純文字之後，才能閱讀。

密碼儲存庫

您的個人密碼的安全儲存區域。它能讓你放心儲存密碼，沒有其他使用者 (甚至是 McAfee 管理員或系統管理員) 可以存取。

掃台者 (wardriver)

配備筆記型電腦、特殊軟體及某些臨時搭載硬體的闖入者，他們在城市、郊外住宅區及商業公園開車四處搜尋，以攔截無線區域網路資料傳輸。

淺層觀察位置

您電腦上的一個資料夾，Data Backup 會監視這個資料夾的變更。如果您設定淺層觀察位置，Data Backup 會備份該資料夾中的觀察檔類型，但是不會包含其子資料夾。

深層觀察位置

在您電腦上由 Data Backup 監視其變更的資料夾 (及所有子資料夾)。如果您有設定深層觀察位置，Data Backup 便會在該資料夾及其子資料夾內，備份觀察的檔案類型。

通訊協定

在兩項裝置之間傳輸資料的協定格式。從使用者的觀點來看，他們對通訊協定唯一感興趣的地方是，如果他們要與其他電腦通訊，其電腦或裝置必須支援正確的通訊協定。通訊協定可部署於硬體或軟體中。

連接埠

資訊進出電腦的地方，例如，傳統的類比數據機是連接到序列埠。TCP/IP 通訊中的通訊埠號碼，是用來將流量分成應用程式特定串流的虛擬值。也會指派標準通訊協定給通訊埠，如 SMTP 或 HTTP，讓程式知道要和哪個通訊埠連線。TCP 封包的目的地通訊埠指出了要尋找的應用程式或伺服器。

十二劃

備份

在安全的線上伺服器建立觀察檔的副本。

惡意存取點

公司沒有授權操作的存取點。麻煩的是，惡意存取點通常都沒有遵守無線區域網路 (WLAN) 安全原則。惡意存取點讓開放式的非安全介面，得以從實際控制的設備之外接觸公司網路。

在適當的安全 WLAN 中，惡意存取點的傷害性比惡意使用者更高。只要設定好有效的驗證機制，未經授權的使用者若要嘗試存取 WLAN，應該是無法順利拿到有價值的公司資源。但是當員工或駭客插入惡意存取點時，就會發生重大問題。只要是在公司網路中配備 802.11 裝置的任何人，惡意存取點幾乎都能容許其進入。如此一來，他們就非常接近重要資源。

無線介面卡

包含電路系統，可讓電腦或其他裝置與無線路由器 (連接至無線網路) 通訊。無線介面卡可內建在硬體裝置的主要電路系統中，或是當作個別的附加元件，透過適當的連接埠來插入裝置。

發佈

將備份的檔案放到網際網路上供人公開存取。

黑名單

被視爲具惡意的網站清單。由於網站從事詐騙活動，或是利用瀏覽器弱點傳送可能無用的程式給使用者，才會將該網站列於黑名單上。

十三劃

節點

與網路連線的單一電腦。

路由器

將封包從一個網路轉送至另一個網路的網路裝置。路由器會根據內部路由表，來讀取每個連入的封包，並決定轉寄的方式。要將連出封包傳送到路由器上的哪個介面，可由任何來源和目的地位址，以及目前的資料傳輸狀況 (例如：負載量、線路價值及不良線路) 的組合來決定。有時亦稱爲存取點 (AP)。

隔離

偵測到可疑的檔案時，便會將其隔離；然後您可以採取適當的行動。

電子郵件

電子郵件 (Electronic Mail) 是透過網際網路或在公司區域網路或廣域網路內傳送的訊息。EXE (執行檔) 檔案或 VBS (Visual Basic script) 檔案格式的電子郵件附件，已普遍成爲傳播病毒及特洛伊病毒 (Trojan) 的途徑。

電子郵件用戶端

電子郵件帳戶。例如：Microsoft Outlook 或 Eudora。

十四劃

漫遊

從一個 AP 覆蓋區移動至另一個區域，而不會中斷服務或連線的能力。

監視位置

Data Backup 在您電腦上監視的資料夾。

網域

網路連線的位址，可在階層格式中識別該位址的擁有者：server.organization.type。例如，從 www.whitehouse.gov 可看出 Web 伺服器在白宮，隸屬於美國政府。

網路

您連接兩部以上的電腦時，便建立了網路。

網路臭蟲

一些小圖形檔案，可以將自己內嵌在您的 HTML 頁面中，允許未授權的來源在您的電腦上設定 Cookie。這些 Cookie 之後便可將資訊傳輸至未經授權的來源。網路臭蟲也稱為網站信標、像素標籤、透明影像圖檔，或看不見的影像圖檔。

網路釣魚

為專門竊取寶貴資訊而使用的詐騙手法，例如：信用卡號碼、社會安全號碼、使用者識別碼及密碼。傳送給可能成為受害者的看起來很正式的電子郵件，會假裝寄件者為受害者的 ISP (網際網路服務供應商)、銀行或零售商。這些電子郵件會傳送給選定名單或是任何名單上的人，希望其中一些收件者剛好真的擁有實際組織的帳戶。

網路圖

於 Network Manager 中，圖形化展現組成家庭網路的電腦與元件。

網路磁碟機

連接至多位使用者共用的網路上之伺服器的磁碟或磁帶機。網路磁碟機有時亦稱為遠端磁碟機。

網際網路

網際網路是由數量龐大、相互連接的網路所組成的，這些網路的定位及資料傳輸都是使用 TCP/IP 通訊協定。網際網路是由美國國防部所創立的大專院校電腦的連結 (1960 年代末期與 1970 年代初期) -- 稱為 ARPANET -- 演變而來的。現今的網際網路是由近 100,000 個獨立網路組成的全球網路。

十五劃

影像分析

防堵可能不當的影像出現。除了成人群組成員之外，系統會防堵所有使用者存取影像。

暴力攻擊法 (brute-force attack)

亦即所謂的暴力破解法 (brute force cracking)，應用程式會以土法煉鋼 (使用暴力) 的嘗試錯誤法來將加密資料 (例如：密碼) 解碼，而非運用智慧型策略來破解。就像罪犯會嘗試各種可能的組合來侵入 (或破壞) 保險箱，暴力破解法 (brute force cracking) 應用程式會依序進行所有可能的有效字元組合來破解密碼。暴力法 (brute force) 雖然耗時，但是絕不失為有效的方法。

標準電子郵件帳戶

大部分家庭使用者都有這類型的帳戶。另請參閱 ＜POP3 帳戶＞。

標題

標題是在訊息的生命週期中，加入至訊息某個部分的資訊。標題會通知網際網路軟體，訊息的傳遞方式、傳送回覆訊息的正確位置、您電子郵件專屬的唯一識別碼，以及其他管理資訊。標題欄位的範例如下：收件者、寄件者、副本、日期、主旨、訊息 ID 及已接收。

潛在的無用程式

潛在的無用程式包括間諜軟體、廣告軟體，以及其他未經您允許而逕自收集和傳輸的資料。

熱點

有存取點 (AP) 透過無線網路來提供公用無線寬頻網路服務給行動訪客的特定地點。熱點通常位於人潮擁擠的地方，例如：機場、火車站、圖書館、碼頭、會議展覽中心，以及飯店等等。熱點的存取範圍通常很短。

線上備份存放庫

位於線上伺服器上的位置，您的觀察檔在備份後，會儲存在此位置。

緩衝區溢位

當可疑的程式或程序嘗試將超過緩衝區限制數量的資料儲存在您電腦上的緩衝區 (暫時資料儲存區)，因而損毀或覆寫相鄰緩衝區中的有效資料時，即會發生緩衝區溢位。

十六劃

整合式閘道

合併存取點 (AP)、路由器及防火牆的裝置。有些裝置亦包含安全加強功能及橋接功能。

頻寬

在固定的時間內能夠傳輸的資料量。若爲數位裝置，通常會以每秒的位元數 (bps) 或每秒的位元組數來表示頻寬。若爲類比裝置，則會以每秒的周數或赫茲 (Hz) 來表示頻寬。

十七劃

壓縮

一種程序，將資料 (檔案) 壓縮成一種格式，使其儲存或傳輸所需的空間減到最小。

檔案庫

Data Backup 使用者所發佈之檔案的線上儲存區域。檔案庫是網際網路上的網站，可供擁有網際網路存取權的任何人存取。

還原

從線上備份存放庫或封存，擷取檔案的副本。

十八劃

瀏覽器

一種用戶端程式，使用超文字傳輸通訊協定 (Hypertext Transfer Protocol，HTTP) 向網際網路中各個 Web 伺服器提出要求。Web 瀏覽器會向瀏覽器使用者呈現圖形式內容。

十九劃

關鍵字

可以指派給已備份檔案的字，以便和指派了相同關鍵字的其他檔案建立關係或連接。為檔案指派關鍵字，可以更容易搜尋您已發佈至網際網路的檔案。

二十劃

攔截式攻擊

攻擊者會中途攔截進行公用金鑰交換的訊息，然後重新傳輸訊息，用它自己的公用金鑰來替換所要求的金鑰，讓原來的二方看起來仍然是直接互相通訊。攻擊者使用一種程式，該程式會讓用戶端以為它是伺服器，讓伺服器以為它是用戶端。攻擊可能單純地只用來取得訊息的存取權，也可以讓攻擊者修改訊息，然後再重新傳輸。這個術語源自球賽，球賽中一些人嘗試直接將球傳給彼此，但中間有一個人企圖搶球。

蠕蟲

蠕蟲是一種會自我複製的病毒，存在於主動式記憶體中，可透過電子郵件訊息來傳送自身的副本。蠕蟲會自我複製並消耗系統資源，進而降低效能或中止工作。

二十三劃

驗證

識別個人的程序，通常是依據使用者名稱及密碼。驗證功能可確保宣稱其身份但提不出存取權的個人。

二十五劃

觀察的檔案類型

Data Backup 備份或封存在觀察位置中之檔案的類型 (例如，.doc、.xls 等)。

關於 McAfee

總部位於加州 Santa Clara 的 McAfee, Inc. 在防護入侵及安全性危機管理上是全球業界的領導者，提供前瞻且經證實的解決方案與服務，並致力於保護全球的系統及網路安全。McAfee 本著無人可及的安全性專業技術並致力於創新之精神，爲家用使用者、企業、公立機構及服務供應商，提供封鎖攻擊、防止破壞以及持續追蹤並改善其安全性的能力。

版權

索引

一劃

四劃

五劃

六劃

七劃

八劃

九劃

十劃

十一劃

十二劃

十三劃

十四劃

十五劃

十六劃

十七劃

十八劃

十九劃

二十劃

二十三劃

二十五劃